EXHIBIT 3

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ANYWHERECOMMERCE, INC. and BBPOS LIMITED, **Plaintiffs,** **v.** **INGENICO, INC., INGENICO CORP., INGENICO GROUP, SA, and INGENICO VENURES SAS,** **Defendants.**	**Civil Docket No: 1:19-cv-11457-IT**

REPLY REPORT OF IVAN ZATKOVICH

TO REBUTTAL REPORT OF DR. SHAMOS

APRIL 18, 2022

CONFIDENTIAL

TABLE OF CONTENTS

LIST OF EXHIBITS

Exhibit No.	Description
A	Curriculum Vitae of Ivan Zatkovich
B	List of Materials Considered
C	Expert Report of Ivan Zatkovich

1 INTRODUCTION

1. I have been retained by Plaintiff BBPOS Limited ("BBPOS"), through its attorneys, Kutak Rock LLP, as an expert in this case. I have previously submitted a report for this case titled Expert Report of Ivan Zatkovich, dated February 16, 2022.

2. This report is a reply to Dr. Shamos' rebuttal report. My qualifications are provided in my previous report. My opinions are based on the information available to me as of the date that I am submitting this report. If additional information becomes available to me either by production by the parties or third parties, or otherwise, I may, if permitted to do so, offer additional opinions. I may also, if requested and permitted to do so, provide further opinions to rebut any testimony, reports or opinions offered by Defendant's witnesses (expert or otherwise). I may present demonstrative or illustrative exhibits at trial to explain my opinions.

1.1 Materials Considered

3. In addition to the materials reviewed in my previous report, I have also reviewed and considered the following references and materials to prepare this response:

- Rebuttal Expert Report of Michael Shamos, PH.D., J.D
- Expert Report of Jennifer Vanderhart, Ph.D.
- Prior art materials asserted by Dr. Shamos

2 BASIC LEGAL PRINCIPLES

4. I requested counsel to review and provide specific responses to the various legal and argumentative criticisms and rebuttals that appear in this section of my report. Unless

otherwise indicated, the legal principles presented herein were supplied to me by counsel to guide my analysis and rebuttal opinions in this report.

2.1 Legal section roadmap

5. The following table is intended to summarize and provide the reader with a roadmap in considering the six primary areas or legal issues that are addressed in this section.

CITATION	DESCRIPTION
2.2	First, a short summary of Dr. Shamos' three criticisms articulated at ¶¶29 and 33-34 of his rebuttal relative to the legal principles at ¶12 of my initial report is provided.
2.3	Second, I discuss my informed understanding of applicable statutory definitions of a trade secret consistent with applicable law and facts and information known in rendering my opinions in this case.
2.4	Third, Dr. Shamos' faulty trade secret determinations based on whether, *theoretically*, BBPOS' trade secrets were susceptible to reverse-engineering are discussed in this section. Rather, the proper inquiry (which he fails to appreciate or address) is whether the trade secrets at issue were, in fact, lawfully acquired by Defendants via actual reverse-engineering or independent development based on sufficient facts or data.
2.5	Fourth, I address Dr. Shamos' unreliable rebuttal opinions and his related third criticism of my report on the issue of whether BBPOS' trade secret theft claims are timely.
2.6	Fifth, pertinent legal principles for determinations of timeliness under Georgia's 5-year statute of limitations that Dr. Shamos' report fails to consider, are presented.
2.7	Finally, I address Dr. Shamos' misapplication of a patentability standard of review by way of prior art references (instead of applicable trade secret legal standards) in rendering his opinions that BBPOS' trade secrets purportedly were publicly available or otherwise commonly or generally known.

2.2 Summary of Dr. Shamos' three criticisms of the "Basic Legal Principles" at ¶12 of my initial report

6. In ¶¶29 and 33-34 of his report, Dr. Shamos offers three main criticisms of my initial report relative to the discussion of pertinent legal principles at ¶12, which was supplied by counsel, summarized as follows:

a) Failure to articulate the statutory definitions of what constitutes a trade secret (at ¶29).

b) Partial omission to the statutory definition of "improper means" under the Georgia Trade Secrets Act, stating: "Reverse engineering of a trade secret not acquired by misappropriation or independent development shall not be considered improper means." O.C.G.A. § 10-1-761(1) (at ¶33).

c) Failure to address whether BBPOS' trade secret theft claims were timely brought within applicable statute of limitations (at ¶34).

7. For the reasons more fully set forth below, I disagree with each of his criticisms, which are a reflection of his own misstatements of and/or faulty applications of controlling legal standards and insufficient facts or data, rather than any objective flaws with legal and factual matters considered in my report, based on the available information known and/or supplied to me.

2.3 All relevant and material legal principles were properly considered and applied in my analysis and determinations on whether BBPOS' IP at issue qualifies for as "trade secret"

8. Prior to my engagement, I had an independent and well-formed understanding of what generally constitutes a "trade secret" under federal and state trade secret theft statutes, which was subsequently confirmed with counsel, post-engagement, to specifically guide my analysis

and all opinions formed in connection with the trade secret theft claims asserted herein under the Georgia Trade Secrets Act, O.C.G.A. 10-1-761, *et seq*., the Massachusetts Trade Secret Act, M.G.L.A. ch.42-42G, and the Defend Trade Secrets Act, 18 U.S.C. § 1831, *et seq*., including, without limitation, each of the opinions set forth in my initial report, herein, or subsequently in this lawsuit, as may be the case.

9. Thus, these applicable statutory definitions (among other relevant legal standards, similarly confirmed or otherwise supplied by counsel), at all relevant times, guided my analysis, and application thereof, to the facts and data perceived by or made known to me for the purposes of rendering expert opinions in the case, in a number of ways, including as a result of independent review and investigation of relevant documentary, tangible, and testimonial evidence in the case; extensive client interviews; independent investigation, inspection, and experimentation with the various devices at issue in the case; discussions with counsel; among others; as well as, generally, through my professional background and expertise in the subject matter. *See, e.g.,* ¶¶1-3, 36, 40-42, 48-50, 52, 62-67, 69-70, 74-117, 189-193, *etc*. (non-exhaustive collection of examples of where my understanding in this regard appears or may have informed certain opinions set forth in my initial report).

2.4 The relevant question is not whether, *theoretically*, a trade secret may be susceptible to reverse-engineering, as Dr. Shamos posits, but, rather, was it, in fact, acquired via reverse-engineering or other lawful means

10. Regarding Dr. Shamos' second criticism at ¶33 of his report (i.e., failing to address the "lawfully acquired" carve-out to the applicable statutory definitions of "improper means" where, among other things, a trade secret may be lawfully obtained by reverse-engineering), I was aware of this legal principle, generally, in reaching the opinions set forth in my report, but

was neither asked to directly opine on this issue in my report, nor on reasonable notice of such assertions by Defendant to possibly address in an anticipatory fashion at the time my report issued.

11. That said, I am informed by counsel, that Dr. Shamos' articulation of this general principle in his report at ¶130[1], and apparent application thereof in his conclusory opinions that that the IP at issue is not trade secret, in part, because it purportedly was susceptible to reverse-engineering, is a misstatement of this legal principle or otherwise reflects a fundamental misunderstanding of how it applies, if at all, in this case.

12. First, I disagree with these opinions for substantive reasons as addressed in my initial report and/or by way of rebuttal herein.

13. Second, I am informed by counsel, that this principle is has a limited application to the claims of misappropriation claims requiring a showing of "improper means" under applicable statutory or case law. Not all acts of misappropriation require it.[2] And, those that do, I understand from counsel, typically consider a defendant's claims that a trade secret was lawfully acquired, such as by reverse-engineering, in the nature of an affirmative defense to be asserted, prosecuted, and then ultimately decided by the fact-finder, in the normal course.

14. Third, I am informed by counsel that, ***the relevant inquiry here, if any, is not***:

---

[1] At ¶130 of his report, Dr. Shamos articulates the applicable standard of review, in relevant part, as follows:

> *. . . A glaring omission from this section is any recognition of the fact that, once a product is sold to the public, any information about its operation that can be ascertained from it by reverse engineering is no longer a trade secret, if it ever was. This is because information that is readily ascertainable by proper means is not a trade secret, and reverse engineering is a proper means under the Georgia Trade Secrets Act, the Massachusetts Trade Secret Act, and the Defend Trade Secrets Act.* (Emphasis added.)

[2] Under the Georgia Trade Secret Act, for example, misappropriation can occur even when the trade secret at issue had been acquired by "accident or mistake" as it is defined at O.C.G.A. § 10–1–761(2). *See Camp Creek Hosp. Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1412 (11th Cir. 1998) (". . . the GTSA includes the diversion of information acquired under legitimate circumstances within its definition of misappropriation, *see* O.C.G.A. §§ 10–1–761(1), 10–1–761(2)(B)(ii)(II) & (III) . . .").

WRONG INQUIRY:	X ***Whether reverse engineering of a trade secret, <u>theoretically</u>, may be possible,***

15. as Dr. Shamos erroneously posits, and then appears to exclusively consider in reaching the opinions on reverse-engineering in his report. Rather, the ***proper question <u>is</u>***:

CORRECT INQUIRY:	***✓ Whether any portion of BBPOS' trade secrets herein were, in fact, lawfully acquired by Defendants via reverse engineering or independent development.***

16. Dr. Shamos' report does not address the latter "correct inquiry," and I am not aware of any efforts having been undertaken by him to analyze and/or formulate any opinions on this issue under this standard based on any facts or information that has been made available to me.

2.5 Dr. Shamos' statute of limitations opinions are unreliable on both legal and factual grounds

17. Dr. Shamos' third criticism of the legal grounds articulated in my report in his rebuttal at ¶34, namely, the listing of applicable statute of limitations periods for BBPOS' trade secret theft claims therein, without offering any direct opinions on the point, is another example of an attempt by Defendants to improperly shift their burdens of production / proof on an affirmative defense to BBPOS.

18. Thus, to the extent this is an issue susceptible to competent expert opinion in this case, it is a matter on which I certainly can (and similarly situated experts normally would) offer rebuttal opinions.

19. At the outset of his report, in the section entitled "SUMMARY OF MY OPINIONS," at ¶¶18-23, Dr. Shamos distills his opinions into six major categories or issues. The sixth area, at ¶23, relates to the timeliness of BBPOS' claims, and states:

> *Mr. Zatkovich has adduced evidence that the claims against Defendants were not brought within any applicable statute of limitations period.*

20. The only other discernable portions of his report that appear to have any relation to Dr. Shamos' dispositive conclusion in ¶23 appear at ¶¶34-36 of his report (and take up about two-thirds of page 10).

21. He cites to (i) *my report* as his purported guidance on the applicable legal principles for determining limitations periods (i.e., five years under Georgia law and three years under both federal and Massachusetts law); (ii) his unsupported "understanding" that BBPOS waited to bring its claims here until sales of its products dried up; (iii) the existence of a September 17, 2012 internal ROAM/Ingenico email communication (referenced in my report at ¶52), between ROAM's Will Graylin and Ingenico's Christopher Rotsaert, that discusses the improper disclosure and theft of BBPOS' IP – a communication to which BBPOS was neither party to nor privy to at the time it was made, but "of which BBPOS had knowledge," he contends without record citation or further detail; (iv) Dr. Shamos, therefrom, goes on to conclude:

> *Given that the longest statute of limitations in this case is five years (Georgia), an action would had to have been brought before September 17, 2017. However, this case was not filed until December 20, 2018, more than a year after expiration of the last statute of limitations.*

22. I note that the limitations periods appearing in my report at ¶12 were supplied to me by counsel, and were neither intended to be or nor otherwise included in my report for any purpose (stated or otherwise) other than to provide some context for pertinent legal principles that I used to guided my own analysis / opinions). I understand from counsel that the legal principles in my report do not present a comprehensive discussion of applicable legal principles for determining when such limitation periods are triggered or subject to tolling (an issue on which I

offered no opinion in my report and involves a complicated mixed legal and factual inquiry, I understand). Nor was my inclusion of these limitations periods in my report intended to be construed as some unspoken invitation for Dr. Shamos' to rely thereon in guiding his opinions or attempt to supplant the Court's role in deciding legal issues.

2.6 Standard of review for determinations of timeliness under Georgia's 5-year statute of limitations

23. In addition to the minimal reference in ¶12 of my report to a five-year statute of limitations applying a trade secret theft claim under Georgia law, I am informed by counsel that the following additional legal principles apply analyzing how to determine when that statute of limitations may be triggered or tolled. These principles, notably, are not addressed by Dr. Shamos in rendering his opinion as to purported timeliness of BBPOS' lawsuit under this statute.

24. The statute of limitations on trade secret claims under the Georgia statute is five years and runs from the time the misappropriation is discovered or, by reasonable diligence, should have been discovered. O.C.G.A. § 10-1-766.

25. Under the "discovery" rule, the statute of limitations does not begin to run until the plaintiff has sufficient information to make a "meaningfully colorable" claim of trade secret misappropriation. The mere suspicion of possible misappropriation does not amount to objectively reasonable notice sufficient to trigger the running of the statute. *Porex Corp. v. Haldopoulos*, 284 Ga. App. 510, 644 S.E.2d 349 (2007), cert. denied, (June 25, 2007).

26. If the plaintiff becomes aware of facts that would make a reasonably prudent person suspicious, he has a duty to investigate further and is charged with knowledge of the matters that would have been revealed in such investigation. This rule applies even if the potential plaintiff

fails to conduct an investigation. However, if certain key facts are unavailable even to a reasonably diligent plaintiff, the statute is tolled until the facts become available. *Id*.

27. Moreover, to prevent multiple claims for a continuing use of a misappropriated trade secret, the statute states that a continuing misappropriation by any person constitutes a single claim against that person. O.C.G.A. § 10-1-766. However, the limitation period is applied separately to claims against different persons who misappropriate the trade secret by receiving it from another misappropriator. *Id*.

28. Mere knowledge that a company is competing in the marketplace and manufacturing similar parts is not dispositive on the accrual of the statute of limitations in a trade secret misappropriation case. *Porex Corp. v. Haldopoulos*, 284 Ga. App. 510, 644 S.E.2d 349 (2007).

29. Guided by these principles accordingly, I disagree with Dr. Shamos' opinion at ¶¶23 and 36 that the statute of limitations on BBPOS' trade secret claims ran on September 17, 2017. My opinion in this regard is based on the facts and information perceived by me or provided to me in this case, including, but not limited to, the fact that, I understand from counsel, BBPOS had no knowledge of this communication alleged to have "triggered" the clock on the 5-year statute of limitations according to Dr. Shamos at ¶36 of his report, until *well after* this lawsuit was filed in 2018 via the parties' exchange of discovery in this case.

30. I also disagree with Dr. Shamos' opinion, summarized at ¶18 of his report, that BBPOS' stolen IP simply "were not" trade secrets. In addition to the commentary and opinions contained in my initial report and as offered elsewhere herein, I note that neither the guiding legal principles (set forth in his report at ¶¶24-36) nor opinions reveal or reflect any indication that Dr. Shamos considered that, in cases where a plaintiff is able to point to a combination, compilation,

or integration of the individual elements of the trade secret that were not publicly disclosed, that information can qualify for protection as a trade secret, notwithstanding the fact that certain aspects of could have been publicly available or otherwise lawfully ascertained, which I am informed by counsel is a legal principle that applies in this case. *See, e.g., Capital Asset Research Corp. v. Finnegan*, 160 F.3d 683, 686 (11th Cir. 1998) (finding that, even when the concept of alleged trade secret information is found to be publicly available, "a unique compilation of that information, which adds value to the information, also may qualify as a trade secret.").

2.7 Dr. Shamos' reliance on a patentability standard of review via prior art references in a trade secret theft case is unavailing

31. Finally, despite outlining certain legal principles at the outset of Dr. Shamos' report at ¶¶24-36, ostensibly, applied by him in analyzing BBPOS' claims of trade secret theft in this case to formulate his opinions, Dr. Shamos instead goes on to devote almost half of his report in the application of a wholly different standard of review – and one that, in my experience and as confirmed with counsel, is typically reserved for determinations of *patentability* rather than trade secret protection – to conclude therefrom that BBPOS' trade secrets were allegedly publicly available.

32. I understand from counsel that, although individual components may be "generally known," this does not necessarily mean the combination of such elements is not trade secret. A court in a trade secret case will need to assess whether a person in the field could discern the information without expending too great an effort (and there is no hard test for this, it is a case-by-case determination). Importantly, this assessment has nothing to do with obviousness. It is about how easy it would be for someone to access the information, *not* how easy it would be for them to come up with the invention contained in that information.

33. I am further advised that the determination of secrecy under a state trade secret theft law is not the same as the PTO's decision whether an invention is obvious in view of the prior art, and it does not follow as a matter of law that something rejected by the PTO as obvious can never be part of a protectable trade secret. Similarly, novelty, in the patent law sense, is not required for a trade secret. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 474-493 (1974). *See also A. O. Smith Corp. v. Petroleum Iron Works Co.*, 73 F.2d 531, 539 (CA6 1934) (emphasizing that, even though a discovery may not be patentable, that does not "destroy the value of the discovery to one who makes it, or advantage the competitor who by unfair means, or as the beneficiary of a broken faith, obtains the desired knowledge without himself paying the price in labor, money, or machines expended by the discoverer.").

34. Finally, I am advised that, although patent rejections based on prior art may be highly persuasive, they are not necessarily determinative of the fact that the claimed trade secret was generally known at the time. *See Celeritas Techs., Ltd. v. Rockwell Intern. Corp.*, 150 F.3d 1354, 1358 (Fed.Cir.1998) (finding that "reliance on the [patent] prosecution history and the prior art submitted to the PTO is misplaced" in upholding a jury verdict of trade secret misappropriation). Regardless of whether a patent application is accepted or rejected, a plaintiff may certainly have a viable trade secret claim where the "implementation details and techniques" or other elements of the trade secret go beyond what was disclosed in the patent. *Id.*; *SkinMedica, Inc. v. Histogen Inc.*, 869 F. Supp. 2d 1176, 1195 (S.D. Cal. 2012).

35. Thus, based on the foregoing legal principles, I also disagree with Dr. Shamos' opinion, summarized at ¶¶18-19 of his report, that BBPOS' stolen IP simply "were not" trade secrets and were "readily ascertainable by proper means." In addition to the commentary and opinions contained in my initial report and as offered elsewhere herein as targeted rebuttal, I note

that neither the guiding legal principles (as set forth in his report at ¶¶24-36) nor opinions reveal or reflect any indication that Dr. Shamos considered these principles in rendering his opinions and, instead, rested on the prior art references found at ¶¶62-164 of his report.

3 SUMMARY OF BBPOS' TRADE SECRETS

36. Of the broad collection of proprietary information that BBPOS has developed since it began developing mPOS devices in 2008, it includes the following asserted trade secrets detailed in this section.

37. The first three trade secrets relate to BBPOS being able to communicate credit card information between an mPOS device and the mobile phone using the audio jack (i.e. headphone / microphone port) on the Mobile phone. This approach allows BBPOS to communicate digital information (and even encrypted information) by converting the digital information to an audio signal to send to the mobile phone audio jack, and then reconverting that audio signal back to digital information in the mobile phone. These methods include developing both circuitry and software on BBPOS' mPOS devices, as well as developing software on the Mobile phone (within BBPOS' SDK application).

38. Although, at the time, it was unusual to communicate digital information to a mobile phone using an audio jack, BBPOS chose this approach because almost every mobile phone has an audio jack. Almost all mobile phones have the ability to plug in a headphone or a headphone with a microphone for listening to music or making phone calls, respectively. In the 2012 time period, many mobile phones did not support Bluetooth, WIFI, or USB communication methods, which would be the traditional means for communicating digital information. Therefore,

BBPOS chose to use the audio jack method and to ensure their ability to use their mPOS devices with as many mobile phones as possible.

39. Because BBPOS utilized this unusual method of communicating digital information from the mPOS device to a mobile phone, they had to develop several proprietary methods and techniques to ensure a reliable communication method. This required much research, investment, and multiple testing trials to understand all possible mobile phone and payment system formats that could be used with an mPOS device. After spending much time, and financial investment, BBPOS was able to design a single configurable solution to address this market situation. Among the proprietary methods they used to ensure reliable communication through an audio jack, BBPOS developed:

1. **Audio Jack Polarity detection –** determines if the base of the mobile phone's audio jack has a positive or negative polarity and to route the microphone/input signal appropriately. This enables a single solution to support multiple mobile phone signal formats.
2. **Power Management –** methods for efficient power use for battery powered mPOS devices as well as performing sleep and auto wakeup (Power on) functions in order to conserve power.
3. **Signal control settings and auto gain control –** determines the appropriate gain (e.g. signal thresholds) to use in decoding data, and at what speed to reliably transmit and receive the information based parameters defined for the specific mobile phone being used.

40. The next two trade secret categories relate to BBPOS' general experience in POS data encryption and their extensive testing and implementation of the many communication formats used by different mobile payment applications. Principally, these are:

4. **Communication Formats –** over 25 different formats for sending credit card and transaction related information between the mPOS device and the mobile phone to ensure compatibility with different mobile payment vendor applications.
5. **Data Security / Encryption methods –** methods for encrypting credit card data based on variations of data encryption methods.

41. These five categories of trade secrets are described in more detail below.

4 SUMMARY OF REBUTTAL RESPONSE OPINIONS

42. The following sections provide details about the opinions in response to Dr. Sha'os' rebuttal report. However, they can be summed up by:

1. None of the prior art Dr. Shamos references discloses the specific details that were provided by BBPOS' trade secrets.
2. The analysis of Ingenico's products indicate they used BBPOS' trade secrets and not the information disclosed in the prior art references.
3. Dr. Shamos indicates that many of the trade secrets could have been reverse engineered. This is incorrect.
4. Dr. Shamos would need to show that Ingenico reverse engineered the BBPOS solutions. He did not.
5. All BBPOS' trade secret information that Ingenico utilized was shared with ROAM/Ingenico.

5 ALLEGED PRIOR ART TO BBPOS' TRADE SECRETS

5.1 Interfacing to the audio jack of a mobile phone

43. Dr. Shamos, in Section VIII. of his rebuttal report, provides sample excerpts from numerous prior art references stating that each indicates that using an audio interface to communicate with a mobile phone was "well-known". However, all of Dr. Shamos' opinions are conclusory. He gives limited or no explanation of how the prior art supports his statements. Nor do any of these documents relate to the BBPOS trade secrets for:

- Polarity Detection
- Power Management
- Automatic Gain Control
- Proprietary Communications Formats
- Security and Encryption formats (Data DUKPT method)

5.1.1 Yasuo et al. Japanese patent application JPH0630153A - filed: 1992

44. In ¶65 of his report, Dr. Shamos states the following only for the Yasuo patent:

> *"Interfacing to the audio jack of a mobile phone was known at least as early as 1992, as disclosed in Yasuo et al. Japanese patent application JPH0630153A, which discloses:*
>
> *In the case of the above item, a terminal with an external communication function is connected to the audio jack I/ F (interface) of the cordless handset, and an experiment using a transfer print system using an external line has been performed and confirmed. In addition, a 4-wire to 2-wire conversion cable has been developed in which a communication modem is built in an information terminal and a modular jack of this information terminal and an audio jack of a mobile (automobile) telephone are connected."*

45. This excerpt comes from the background section and refers to some other prior art as an example. The Yasuo patent simply discusses the general concept of connecting a cordless

phone to a printer. It relies on traditional audio data transmission standards of a landline facsimile machine. This not the same method of encoding digital data through the audio jack of a cell phone developed by BBPOS which was then shared with and used by Ingenico and Roam. The method for transmitting facsimile information is only appropriate for sending raster images, not credit card data and numerical information.

46. Specifically, Yasuo lacks any information regarding:

- How to implement two-way encoded data communication using the microphone and L and R channels of a stereo audio jack. Yausuo's headset interface of a landline based cordless phone is different than the audio jack of a cell phone.
- Any detail on how to encode or decode the data from the audio tones using a cell phone audio jack.
- What speed of and type of transmission to use for which phones (BBPOS identified the specific settings and configurations for more than 442 different cell phone models.
- A solution for the inconsistent gain of the different types of cell phones that cause communication errors and data loss.
- A solution to protect the device from the reversed polarity of certain cell phone audio jacks.

47. Yasuo provides no specific circuits, algorithms, or communication formats for communicating credit card transaction information over a cell phone audio jack that BBPOS provided.

48. In many cases BBPOS was providing solutions to problems that Ingenico / Roam were not even aware existed in mPOS devices. This is evidenced by:

- Multiple emails between the BBPOS, Roam Data and Ingenico teams regarding Polarity Detection, Power Management and Communication Formats which include using the Data DUKPT method, as shown in detail in Section 6.2 including:

  - *Email string between Mr. Rotsaert and BBPOS Engineer Daniel Tsai regarding the Power Management trade secret:Power Power Management [IngenicoInc_0048390-IngenicoInc_0048391]*

  - *Communication Format and the Audio Interface design, including power management circuit. [BBPOS_0005630]*

    Attached Documents:
    - *Phone list.xlsx [BBPOS_0005631]*
    - *BBPOS-DataOutputFormat-V1.15.doc [BBPOS_0005633-BBPOS_0005645]*
    - *audio interface.pdf [BBPOS_0005632]*

  - *Paypal Schematic which shows both the Polarity circuit and the Power Management circuit design, the EMV Flow, Two Communications, and Output Format v1.21 which also relies on use of the Data DUKPT method. [IngenicoInc_0009651]*

    Attached Documents:
    - *BBPOS EMVFlow.docx [IngenicoInc_0009626-IngenicoInc_0009627*
    - *BBPOS TwoWayCommunication.docx [IngenicoInc_0009628-IngenicoInc_0009629]*
    - *BBPOS-DataOutputFormat-V1.21.doc [IngenicoInc_0009636-IngenicoInc_0009650]*
    - *Paypal-PCB1-ST04-V3.1.pdf [IngenicoInc_0009622-IngenicoInc_0009624]*

- Multiple emails between BBPOS, Roam Data and Ingenico teams regarding AGC and Shared SDKs with Roam data which include Communication Parameter Setting and AGC, as shown in detail in Section 6.5 including:

    - *SDK code shared with Roam Data team [BBPOS_0004844]*
    - *Discussion of Testing of SDKs between BBPOS, Roam & Ingenico teams [BBPOS_0651362]*
    - *Planning of next SDK release between BBPOS, Roam & Ingenico teams [BBPOS_1633041]*

- *Multiple emails between BBPOS, Roam Data and Ingenico teams regarding Data Output Formats, as shown in detail in Section 6.6 including:*

    - *BBPOS Engineer, Daniel Tsai, provided BBPOS-DataOutputFormat-V1.15.doc on July 16, 2012 to Christopjer Rotsaert. [BBPOS_0005649-BBPOS_0005663]*
    - *BBPOS Engineer, Daniel Tsai, provided BBPOS-DataOutputFormat-V1.21.doc on July 17, 2012 to Christopjer Rotsaert. [BBPOS_0005649-BBPOS_0005663]*

- *Multiple emails between BBPOS engineers and Ingenico engineers regarding Data DUKPT method, as shown in detail in Section 6.7 including:*

    - *String of emails including the one below between BBPOS Engineer, Jimmy Tang, and Ingenico Engineer, Jerome Grandemenge, regarding the implementation of the DUKPT method for integrating with the Ingenico devices.*
        - *Sends Data DUKPT code [BBPOS_0004382]*
        - *Troubleshooting of Data DUKPT [BBPOS_0004428-BBPOS_0004430]*

5.1.2 Nanikashvili U.S. Patent 7,452,878 – filed: 2005

49. In ¶66 of his report, Dr. Shamos states the following only for the Nanikashvili patent:

> *"Further, it was known to use the audio jack of a mobile phone to interface to medical monitoring devices. For example, Nanikashvili U.S. Patent 7,452,878, filed February 16, 2005, discloses at 3:29-43:*
>
> *A cellular phone that does not include a short-range transceiver, such as a bluetooth transceiver can be connected to an adapter or other means that facilitates short-range communication with the phone. U.S. patent application 2003/0045235 of Mooney et al. describes a smart bluetooth interface gate way device that allows a bluetooth headset to establish an audio connection and communicate with a conventional wireless phone (e.g., a wireless phone that does not have bluetooth installed). The connection is controlled merely by monitoring the presence of* ***sound and tones in the audio stream from an analog audio jack of a conventional wireless phone****. The smart bluetooth interface gateway device is attached to the wireless phone just as a wired headset would. Use of the wireless phone is the same as if a wired headset were plugged in."*

50. For reference, it should be noted that the Nanikashvili Patent is 7,542,878 not 7,452,878 as referred to by Dr. Shamos.

51. The only disclosure in Nanikashvili as to how to communicate between a cell phone and a device using an analog audio jack, are these three sentences in the background section referencing a patent from Mooney et al U.S. Patent Application Publication 2003/0045235, published March 6, 2003.

> *"The connection is controlled merely by monitoring the presence of sound and tones in the audio stream from an analog audio jack of a conventional wireless phone. The smart bluetooth interface gateway device is attached to the wireless phone just as a wired headset would. Use of the wireless phone is the same as if a wired headset were plugged in."*

52. There is no other information in Nanikashvili as to how to design, develop, or implement this interface. Therefore, it is lacking any information regarding:

- How to implement two way encoded data communication using the microphone and L and R channels of a stereo audio jack (other than Nanikashvili indicating that it is an analog audio port).
- Any detail on how to encode or decode the data from the audio tones transmitted on the cell phone audio jack.
- What frequencies or speed of transmission to use, what speeds to use for which phones (i.e. BBPOS identified the specific settings and configurations to use for more than 442 different cell phone models)
- A solution for the inconsistent gain of the different types of cell phones that cause communication errors and data loss.
- A solution to protect the device from the reversed polarity of certain cell phone audio jacks.

53. The Mooney patent speaks to a Bluetooth gateway that allows a Bluetooth headset to attach to a cell phone that does not have blue tooth capabilities in order to make phone calls. This is not the same as using an mPOS device with an audio jack of a mobile phone. In addition, there is no discussion in Mooney of how to handle solve the Polarity Detection, Power Management or Automatic Gain Control as addressed in the BBPPS mPOS device.

54. Therefore, Mooney does not disclose the trade secret information that BBPOS provided to Roam and Ingenico regarding these BBPOS trade secrets.

5.1.3 Other Prior Art using an audio jack of a mobile phone

55. Additionally, Dr. Shamos provides a list of other prior art that refers to connecting something to a cellular phone's audio jack. He describes this list as showing that it was not unusual to connect devices to mobile phones. However, there is little or no explanation of how

these compare to, or teach, the trade secrets used in the BBPOS devices that were shared with ROAM/Ingenico and Landi. None of the prior art listed describe:

- How to implement two way encoded data communication using the microphone and L and R channels of a stereo audio jack (other than Nanikashvili indicating that it is an analog audio port).
- Any detail on how to encode or decode the data from the audio tones transmitted on the cell phone audio jack.
- What frequencies or speed of transmission to use, what speeds to use for which phones (i.e. BBPOS identified the specific settings and configurations to use for more than 442 different cell phone models)
- A solution for the inconsistent gain of the different types of cell phones that cause communication errors and data loss.
- A solution to protect the device from the reversed polarity of certain cell phone audio jacks.

56. The prior art asserted by Dr. Shamos in support of interfacing to the audio jack of a mobile phone is simply a list of documents where the audio jack of a mobile phone is used for some purpose other than performing a POS operation. No attempt is made to show they could possibly resemble the capabilities of an mPOS device interfacing to a mobile phone. Dr. Shamos presents this list of conclusory prior art:

- Challa et al. U.S Patent 7,857,225 – filed: 2007
- Cehelnik U.S. Patent Application Publication 2006/022910 – published: 2006. For reference, it should be noted that the Cehelnik Patent is US20060229108A1 not 2006/022910 as referred to by Dr. Shamos.

- Son et al. U.S. Patent Application Publication 2008/0004894 – published: 2008
- Griffin, Jr. U.S. Patent Application Publication 2010/0184479 - published: 2010
- Pennock et al. U.S. Patent Application Publication 2012/0008851 - published: 2012
- Pennock et al. U.S. Patent Application Publication 2012/0011071 - published: 2012
- Mu et al. U.S. Patent Application Publication 2012/0052910 - published: 2012
- On October 13, 2010 Dorsey (a founder of Square) filed an application that was published on April 21, 2011 as International Publication Number WO 2011/047042
- Shadwell Jr. et al. U.S. Patent Application Publication 2012/0061462 - published: 2012
- Tekin et al. U.S. Patent Application Publication 2012/0100887 - published: 2012

57. I disagree. I do not see where any of this prior art discloses BBPOS' trade secrets regarding Polarity Detection and Correction, Power Management or the Adaptive Threshold method for Automatic Gain Control as the BBPOS devices were designed to do.

5.2 Prior Art relating to BBPOS' Audio Jack Polarity Detection design

58. In ¶82 of his report, Dr. Shamos claims that the BBPOS solution for Polarity Detection and Correction could be found through reverse engineering the BPPOS device.

> *"Any solution to polarity detection embodied in any BBPOS circuit could be readily ascertained by reverse engineering."*

59. I disagree. Even though some of the BBPOS circuit designs appear simple in hindsight, these designs have been highly refined and simplified for cost effectiveness over many iterations. And some of those many design iterations were shared with Ingenico.

60. In addition, dissecting BBPOS' circuit boards, and even probing the signals of an operating BBPOS device, would only reveal that there are circuits containing transistors, for example, between the audio jack signals and the rest of the mPOS device. There would be no indication as to the purpose of those circuits or why Ingenico would want to incorporate them into their designs.

61. As shown by my analysis below, none of Dr. Shamos' references to the alleged prior art provided any level of detail that would have allowed Ingenico to implement circuits that would have been close to the simplicity and effectiveness of BBPOS' designs, where the circuit would both detect and automatically correct the polarity with minimal low cost components (i.e. a couple transistors). To the contrary, the only prior art that Dr. Shamos cited would have performed roughly the same function as the Texas Instruments specially designed chip. And this would have not revealed the actual design of the circuit and would have been significantly more expensive than BBPOS' solution.

5.2.1 Wenger does not disclose BBPOS' trade secrets regarding Polarity Detection and Correction

In ¶84 of his report, Dr. Shamos claims that Wenger discloses a solution for polarity detection and correction.

> *"The use of MOSFET transistors for polarity detection was disclosed in Wenger U.S. Patent 6,703,822 ("Wenger"), which issued March 9, 2004, entitled, "Circuit for Detecting a Current Passing Through a Consumer":*
>
> ***A very advantageous embodiment of the invention has turned out to be one in which the power output stages of the amplifiers are comprised of MOSFETs**, which function in push-pull B operation. In this connection, it is*

> *very advantageous if the power output stages of the amplifiers are each triggered by means of an operational amplifier that the output of the relevant power output stage is coupled back to. In an embodiment of this kind, it is very useful that the supply voltage of the operational amplifier is higher than the operating voltage of the circuit arrangement, as a result of which the power output stage transistors can be controlled in a fully advanced manner."*

62. Dr. Shamos is incorrect. The Wenger invention is not related to the detection or correction of the polarity of an audio signal in a cell phone audio jack or any audio interface. It discusses the provision of a proper supply voltage to a generic signal amplifier circuit.

63. The only mention of polarity detection is for the purpose of evaluating "voltage between the two branches of the bridge exciter". This solution does not apply to detecting the polarity of audio jack signals and would provide no value when developing a communication method between an mPOS device and a cell phone.

64. Therefore, Wenger does not disclose BBPOS' trade secrets regarding Polarity Detection and Correction between a cell phone and an mPOS device using an audio jack interface and does not provide the solution performed by BBPOS' trade secrets.

5.2.2 Yi does not disclose BBPOS' trade secrets regarding polarity detection and correction

65. Then, in ¶85 of his report, Dr. Shamos claims that the Yi patent discloses a solution for polarity detection and correction.

> *"The need for polarity detection and correction was disclosed in Yi et al. U.S. Patent 6,809,572 ("Yi"), issued on October 26, 2004 and entitled, "Integrated Circuit with Automatic Polarity Detection and Configuration." It teaches:*
>
> *An integrated circuit on a system board is used, for example, in a digital audio device (such as a DVD or NV receiver). The integrated circuit includes a digital-to-analog converter and the system board may include circuitry to mute the analog output of the device under certain predefined conditions.* ***Because it may not be known in advance by the designer of the integrated circuit whether the circuit is activated by a signal in a high state (polarity) or a low state, the integrated circuit includes a detector which detects and stores the***

> ***required polarity. When it is necessary for the circuit to be activated, the detector provides a signal of the correct polarity.***"

66. This, too, is incorrect. The Yi invention has nothing to do with detecting and reversing the polarity of an analog audio signal. The purpose of Yi is to provide a circuit to mute the audio output. Additionally, it allows the mute circuit to be enabled automatically with either a "high" signal or "low" signal.

67. The polarity of the audio signal itself remains unchanged. The circuit identified in Dr. Shamos' report, and the other circuits described in the Yi patent, are used merely to mute or unmute the audio output, not detect or change its polarity.

68. Therefore, Yi does not disclose BBPOS' trade secrets regarding polarity detection and correction between a cell phone and an mPOS device using an audio jack interface and does not provide the solution performed by BBPOS' trade secrets.

5.2.3 Cehelnik does not disclose BBPOS' trade secrets regarding Polarity Detection and Correction

69. And, in ¶87 of his report, Dr. Shamos cites to the Cehelnik patent which he claims discloses a solution for polarity detection and correction:

> *"The need for polarity detection and correction was also disclosed in Cehelnik (referenced above) at [0054]:*
>
> *The mobile phone is the demonstration is an LG4400, but other phones will work fine if the headset jack is wired the same.* ***For noncompliant cases, the circuit is generally applicable, just the pin connections needs reordered****. FIG. 2 shows a 2.5 mm male stereo phone jack 18 that is used to connect the phone extension interface card 56 to the mobile phone female headset jack 19. FIG. 3 shows 1/8 inch stereo phone jack 82 used to connect the phone extension interface card 56 to the basestation headphone jack."*

70. Note: Cehelnik is U.S. Patent Application Publication 2006/0229108 not 2006/022910 as referenced in Dr. Shamos' report.

71. Dr. Shamos' assertion is not correct. As described in the abstract, Cehelnik is not related to the detection or correction of the polarity of an analog audio signal. The purpose of the invention is simply to relay the audio signal received on a landline phone to a cell phone to be transmitted on the cellular network. The sentence that Dr. Shamos cites to in Cehelnik is merely stating that the pins for a landline headset need to be connected correctly to the pins of the mobile phone audio jack. This is evident by the reference in Cehelnik, stating:

> ***"For noncompliant cases, the circuit is generally applicable, just the pin connections needs reordered"***

72. There is no mention anywhere in Cehelnik that there is even a need to detect or correct the polarity of the audio signal sent to or received from a cell phone.

> *A method and apparatus is present for achieving simple and inexpensive communications from wired phones to mobile or cell phones called a mobile phone extension. It is inexpensive because of flexible system architecture and simple hardware implementation. It allows phone calls to be made from wired phones over a cell phone.* ***It is simple because audio signals from a microphone and speaker of a wired handset are connected to the mobile phone via a simple plug connection to the headset audio port****. ... [Cehelnik abstract]*

73. Therefore, Cehelnik does not disclose BBPOS' trade secrets regarding polarity detection and correction between a cell phone and an mPOS device using an audio jack interface and does not provide the solution performed by BBPOS' trade secrets.

5.2.4 Poulson does not disclose BBPOS' trade secrets regarding Polarity Detection and Correction

74. In ¶88 of his report, Dr. Shamos indicates that Poulson discloses a solution for polarity detection and correction.

> *"The need to detect polarity of a device plugged into the audio jack of a mobile phone was also disclosed in Poulsen et al. U.S. Patent Application Publication 2012/0134503 ("Poulsen"), entitled, "System and Method for Microphone*

> *Polarity Detection," published May 31, 2012. Poulsen provides solutions to the problem, including circuits and flowcharts. The Poulsen abstract discloses:*
>
> *The present disclosure provides a method of determining microphone polarity in a headset. By being able to detect the polarity of the microphone within the headset, a portable electronic device may be compatible with any headset and is not limited to use with a specific headset.* ***By applying a detection signal over one of lines within a headset cable, a return signal may be sensed on one of the other lines to determine which of the lines is the ground line and which line is the microphone line****."*

75. The Poulsen application does identify one method for detecting the polarity of the microphone signal in the headset connected to a mobile phone. However, it uses a different method than that developed by BBPOS. The Poulsen method requires sending a separate artificial test signal that must be synchronized and detected by the receiving end. The circuitry disclosed in Poulsen in no way relates to the several circuit designs shared by BBPOS with Ingenico and Roam. In addition, the Poulsen method also does not disclose how to automatically correct the polarity of the audio signal.

76. The method developed by BBPOS does not need an artificial test signal. BBPOS designed circuitry that automatically detects the polarity of the audio signal during normal operation of the interface, as well as automatically correcting the polarity of that signal, if needed. This was the design that BBPOS shared with, and was used by, Ingenico and Roam.

77. Therefore, Poulson does not disclose BBPOS' trade secrets regarding polarity detection and correction between a cell phone and an mPOS device using an audio jack interface and does not provide the solution performed by BBPOS' trade secrets.

5.2.5 Texas Instruments' product does not disclose BBPOS' trade secrets regarding Polarity Detection and Correction

78. In ¶¶89-90 of his report, Dr. Shamos cites to a specially designed chip offered by Texas Instruments which he claims performs polarity detection and correction.

"By 2012, Texas Instruments was offering a device, the TS3A225E "Autonomous Audio Headset Switch," that detected the polarity of a device connected to an audio jack, described in a TI data sheet[4] as follows:

The TS3A225E is an audio headset switch device. The device detects the presence of an analog microphone and switches a system analog microphone pin between different connectors in an audio stereo jack. The microphone connection in a stereo connector can be swapped with the ground connection depending on manufacturer. When the TS3A225E detects a certain configuration, the device automatically connects the microphone line to the appropriate pin. The device also reports the presence of an analog microphone on an audio stereo jack.

The TI circuit includes two MOSFET transistors:"

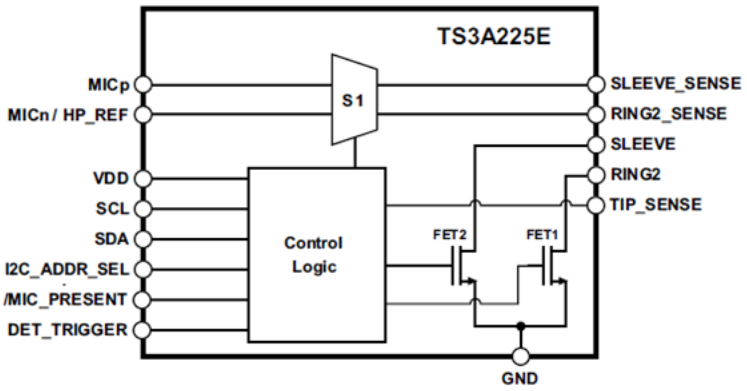


Figure 1. Functional Block Diagram

79. The Texas Instruments datasheet describes a specially designed integrated circuit (chip) to perform the polarity detection of the microphone signal from an audio stereo jack. The description of this specially designed chip does not indicate how this polarity detection is performed other than indicating that "control logic" will provide the correct microphone signal to the output pin of the chip.

80. Further, the TI chip is actually designed to be used for the mobile phone side of the signal and would not be applicable for an mPOS device. For example, the power requirements for the TI chip would be more than BBPOS' more efficient design. Also, the chip form factor is too large to be used in the slim format required for the mPOS devices.

81. BBPOS not only provided specific information to Ingenico and Roam as to how to detect and correct the polarity of the audio signal, but they provided several specific circuit designs to do that. In addition, the information and designs provided by BBPOS would have been significantly cheaper than the purchase of a specialty chip designed and sold by Texas Instruments. A volume price for the TI chip is approximately $0.35, whereas the two transistor design of BBPOS would be less than $0.04.

82. The TI chip would not only be directed at the cellphone side of the audio jack interface, it would be incompatible with the size and operating requirements of the mPOS device, not to mention a much more expensive alternative even if it were compatible.

83. Therefore, the Texas Instruments' TS3A225E product does not disclose BBPOS' trade secrets regarding polarity detection and correction between a cell phone and an mPOS device using an audio jack interface and does not provide the solution performed by BBPOS' trade secrets.

5.3 Prior Art relating to BBPOS' Power Management design (Auto Power On)

84. In ¶95 of his report, Dr. Shamos claims that the elegant BBPOS power management design could be achieved by reverse engineering. If that were the case, Ingenico would not have needed to request so much information about power management and battery life from BBPOS. Dr. Shamos only makes this statement and nothing else to justify this claim.

> *"Any power management facilities embodied in any circuit in a BBPOS product could be readily ascertained by reverse engineering."*

85. This statement is not correct. Although it may have been possible to determine the intent or purpose of some of the aspects of BBPOS' power management designs, some aspects of the design were implemented by internal logic within the microprocessor code for example. And

this information would not be readily detectable, even in light of the alleged prior art referenced by Dr. Shamos. Specifically, none of the prior art disclosed these aspects of BBPOS' trade secrets that were shared with Ingenico and Roam, that is:

- specific circuitry used to detect activity on the audio jack,
- specific circuitry used to wake up the microprocessor and keep the power on until the microprocessor could verify the audio signal, and
- the logic to have the microprocessor analyze the audio signals, and if the signals were not valid mPOS signals, to immediately turn off the power again.

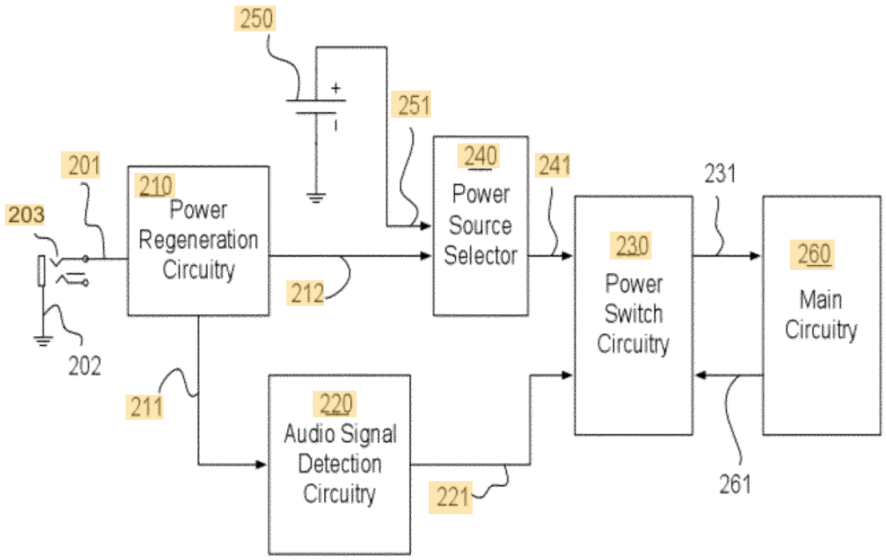
5.3.1 BBPOS' patents (e.g. Chan) do not disclose the Power Management Circuitry Trade Secret

86. In ¶101 of his report, Dr. Shamos states that BBPOS patents disclosed the trade secret for Power Management circuitry, meaning it would wake up a device based on activity on the circuit and then turn off the device if the activity was not characteristic of an mPOS signal.

> *"Having devices sleep to conserve power and wake on activity was well-known in the field. For example, BBPOS itself made the information public in Chan et al. U.S. Published Patent Application 2012/0293001 ("Chan"), entitled "Power Management Circuitry in Peripheral Accessories of Audio Devices," published November 22, 2012. It discloses:*
>
> *In general, in one aspect the invention provides a power management circuitry that is used in a peripheral electronic device. The power management circuitry includes a power regeneration circuitry, a power selector, a power switch and an audio signal detection circuitry. The power regeneration circuitry is configured to receive a continuous periodic sound wave from an audio device and to convert the continuous periodic sound wave into an amplified DC electrical signal. The power source selector is configured to receive a first input comprising the amplified DC electrical signal from the power regeneration circuitry and a second input from a primary power source and to provide a power signal output. The audio signal detection circuitry is configured to receive the amplified DC electrical signal from the power regeneration circuitry and to transmit a wake-up signal to the power switch circuitry.* ***The power switch circuitry is configured to be turned on by the wake-up signal and to connect the power source selector to the peripheral***

electronic device main circuitry and thereby to transfer the power signal output to the peripheral electronic device main circuitry."

87. I disagree. The BBPOS Chan patent describes a method for power management that provides both a wake-up signal and a method to harvest the power present in the audio signal to assist in charging the battery. However, the information disclosed in the patent primarily discusses this concept in functional blocks not in specific circuitry (see Chan fig. 2 below).



88. The only specific circuitry identified in the Chan patent identifies the voltage doubling diodes that are used to harvest the power within the audio signal. This aspect of the design was not utilized by Ingenico or Roam. The trade secret provided by BBPOS to Ingenico and Roam included:

- specific circuitry used to detect activity on the audio jack,
- specific circuitry used to wake up the microprocessor and keep the power on until the microprocessor could verify the audio signal, and

- the logic to have the microprocessor analyze the audio signals, and if the signals were not valid mPOS signals, to immediately turn off the power again.

89. None of these aspects of the power management trade secret, that was shared with Roam and Ingenico, are disclosed in the Chan patent. Yet Ingenico and Roam utilized all 3 of these design aspects shared by BBPOS in their product design.

5.3.2 Lam does not disclose the BBPOS Power Management Trade Secret

90. Dr. Shamos also asserts the Lam patent 5,822,598 by stating in ¶102 *"Further, the idea of such power management is even older."* Dr. Shamos claims it discloses the detection of audio activity to increase battery life of portable computers which he asserts is the same as the BBPOS Power Management design.

> *A power management system for a computer system having an audio circuit which generates an audio output signal. An activity detection circuit senses audio signal activity on the analog audio signal. The power management system maintains power to at least the audio circuit when activity is detected on the analog audio circuit by the activity detection circuit.* ***The power management system causes the audio circuit to enter a power conservation mode when no activity is detected by the audio detection circuit on the audio analog signal for a predetermined amount of time****. Lam, Abstract*

91. This is incorrect. The concept presented by Lam simply looks for activity on the analog audio circuit over a period of time. If there is no activity, the device is powered off, if there is some activity, the device is powered on. It does not interrogate data in the signal to determine if it is activity from audio signals encoded with specific mPOS commands and card transaction data. BBPOS provided to Roam and Ingenico:

- specific circuitry used to detect activity on the audio jack,
- specific circuitry used to wake up the microprocessor and keep the power on until the microprocessor could verify the audio signal, and

- the logic to have the microprocessor analyze the audio signals, and if the signals were not valid mPOS signals, to immediately turn off the power again.

92. None of these aspects of power management are disclosed in the Lam patent. Yet Ingenico and Roam utilized all 3 of these design aspects shared by BBPOS in their product design.

5.3.3 Fiennes does not disclose the BBPOS Power Management Trade Secret

93. In ¶103 of his report, Dr. Shamos describes the Fiennes patent as disclosing the Power Management Circuitry by powering on, and off, electronic devices if there is, or is not, some activity, respectively.

> *"Fiennes et al. U.S. Published Patent Application 2009/0307511 ("Fiennes"), entitled "Portable Electronic Devices with Power Management Capabilities," was published on December 10, 2009. It discloses:*
>
> *When the electronic device is in the standby mode and activity is detected, the codec may be configured to provide an interrupt signal to a power management unit that wakes the device. When the electronic device is in active mode and no user inputs are received within a given period of time, the central processor in the electronic device may place the device in standby mode."*

94. The Fiennes patent describes a power management method that detects activity on one of several inputs to the device including the audio signals to/from the headset. However, there is no specific circuitry identified to perform this function only general logical blocks as illustrated in Fig. 5 of Fiennes.

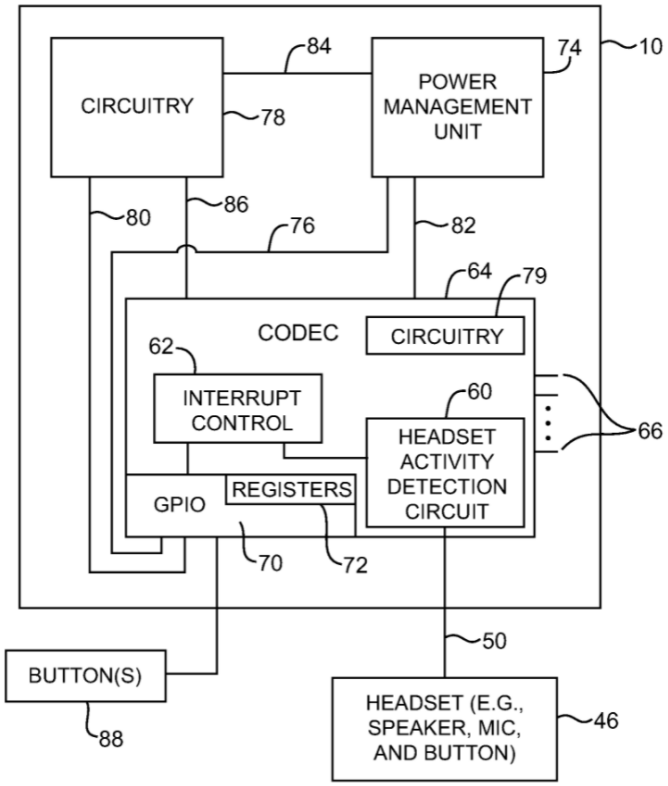


FIG. 5

95. In addition, Fiennes discusses the detection of activity from straight analog audio signals such as voice and music, rather than detecting activity from audio signals encoded with specific mPOS commands and card transaction data. BBPOS provided to Roam and Ingenico:

- specific circuitry used to detect activity on the audio jack,
- specific circuitry used to wake up the microprocessor and keep the power on until the microprocessor could verify the audio signal, and
- the logic to have the microprocessor analyze the audio signals, and if the signals were not valid mPOS signals, to immediately turn off the power again.

96. None of these aspects of power management are disclosed in the Fiennes patent. Yet Ingenico and Roam utilized all 3 of these design aspects shared by BBPOS in their product design.

5.3.4 Walsh does not disclose the BBPOS Power Management Trade Secret

97. In ¶104 of his report, Dr. Shamos describes the Walsh patent as disclosing the Power Management Circuitry.

> *"Walsh et al. U.S. Published Patent Application 2011/0167287, entitled "Providing Power to an Accessory During Portable Computing Device Hibernation," was published on July 7, 2011. It discloses:*
>
> *A portable computing device (PCD) can selectively supply power to an accessory during PCD hibernation. In some embodiments, the PCD's **default behavior is to disable accessory power output during hibernation**, and this default behavior can be overridden in response to a request from a connected accessory. **The accessory can use the power supplied during PCD hibernation to detect user input (or other) events and wake the PCD from hibernation in response to a detected event**. Some accessories can wake the PCD by emulating accessory detachment and reattachment."*

98. The Walsh patent application is a very generic method describing the 'hibernation' and 'waking up' of a portable computing device, such as a laptop, and/or it's peripherals. This occurs when the portable device detects the user is providing input (e.g. typing on the keyboard, touching the touchpad or touchscreen, speaking into the microphone, etc.). Walsh does not disclose any specific methods or circuitry for detecting activity from a microphone for example. Nor does Walsh disclose any information regarding if, or how, the portable device should determine if the activity from the microphone was valid activity in order to remain awake or go back into hibernation.

99. BBPOS provided to Roam and Ingenico:

- specific circuitry used to detect activity on the audio jack,

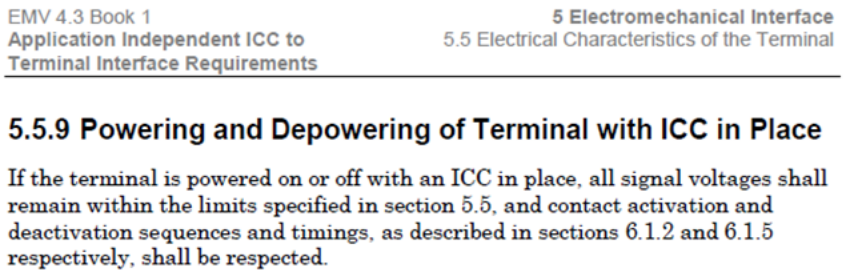
- specific circuitry used to wake up the microprocessor and keep the power on until the microprocessor could verify the audio signal, and
- the logic to have the microprocessor analyze the audio signals, and if the signals were not valid mPOS signals, to immediately turn off the power again.

100. None of these aspects of power management are disclosed in the Walsh patent. Yet Ingenico and Roam utilized all 3 of these design aspects shared by BBPOS in their product design.

5.3.5 The EMV Standard does not require the BBPOS Power Management Trade Secret

101. In ¶106 of his report, Dr. Shamos claims the EMV Standard requires this type of Power Management Circuitry designed by BBPOS.

> *"The ability to turn an interface on or off, which BBPOS asserts to be a trade secret, was in fact a published EMV requirement. The images below are from the "EMV Integrated Circuit Card Specifications for Payment Systems Book 1" (2011)[5]:"*



EMV 4.3 Book 1
Application Independent ICC to Terminal Interface Requirements

5 Electromechanical Interface
5.5 Electrical Characteristics of the Terminal

5.5.9 Powering and Depowering of Terminal with ICC in Place

If the terminal is powered on or off with an ICC in place, all signal voltages shall remain within the limits specified in section 5.5, and contact activation and deactivation sequences and timings, as described in sections 6.1.2 and 6.1.5 respectively, shall be respected.

102. This is incorrect. The EMV requirement document referenced by Dr. Shamos simply describes the operating characteristics (e.g. voltages) of the EMV device when it is powering up, operating, and powering down. It provides no information as to what criteria causes the "powering and depowering" of the device. Nor does it provide for the testing of valid input signals in order to trigger the device state.

103. BBPOS provided to Roam and Ingenico:

- specific circuitry used to detect activity on the audio jack,
- specific circuitry used to wake up the microprocessor and keep the power on until the microprocessor could verify the audio signal, and
- the logic to have the microprocessor analyze the audio signals, and if the signals were not valid mPOS signals, to immediately turn off the power again.

104. None of these aspects of power management are disclosed in the EMV requirements. Yet Ingenico and Roam utilized all 3 of these design aspects shared by BBPOS in their product design.

5.4 Prior Art relating to BBPOS' Pre-analyzed communication settings and adaptive threshold (or Auto Gain Control)

105. In ¶¶108-109 of his report, Dr. Shamos claims the aspects of this trade secret would be easily obtained through reverse engineering.

> *"In ¶65, Mr. Zatkovich says that the communication settings trade secret "determines the appropriate gain (e.g. signal thresholds) to use in decoding data, and at what speed to reliably transmit and receive the information based parameters defined for the specific mobile phone being used." More details of this supposed trade secret are found in ¶¶ 85-99.*
>
> *Any adaptive threshold facilities embodied in any BBPOS circuit could be readily ascertained by reverse engineering. Ingenico had no access to the source code of the BBPOS SDK, so any adaptive threshold facilities resident in that code was not available to Ingenico."*

106. This is not correct. The specific algorithm for the adaptive threshold method as I describe in my report, is an internal algorithm used by the processor to determine the signal threshold that identifies when the next "bit" of data can be detected. There are no outward indications of how this method works or how the processor is making those adjustments. The

operation and results of this method occurs purely within the code. Therefore, it would not be possible to reverse engineer the adaptive threshold method.

107. In addition, BBPOS shared code from their SDK with Roam that Ingenico could have utilized regarding communications settings.

108. BBPOS shared information with Ingenico describing its method of Automatic Gain Control. In several emails between BBPOS and Ingenico's Mr. Rotsaert, BBPOS engineers described how they adjusted the data rate, for example, to produce a more reliable signal. Because,

> *"The AGC (automatic gain control) of every phone behaves differently and it affects the received signal quality." [BBPOS_1396262-BBPOS_1396263]*

109. In ¶110 of his report, Dr. Shamos claims that anyone in the industry could obtain BBPOS' communication parameters used to properly configure the communication settings for over 400 different models of mobile phones.

> *"In ¶ 92, Mr. Zatkovich refers to BBPOS' analysis of 11 different parameters for 442 phone models. By their very nature, these parameters were readily ascertainable from the phones themselves, and cannot constitute a trade secret of BBPOS. Anyone in the industry could obtain these parameters, which contain no BBPOS information. Further, Mr. Zatkovich furnishes no evidence that the values of these parameters were ever disclosed to Ingenico."*

110. It is possible that some of the 11 different parameters and communication settings could be ascertained by Ingenico through reverse engineering after exhaustive monitoring of the signals that BBPOS generated between the various models of mobile phones and the mPOS devices. However, some of the parameter settings used by Ingenico such as AudioSource could not be determined through monitoring of signals since this occurs only within the software and has no externally detectable indications.

111. In addition, some of the parameters could be ascertained only approximately by monitoring BBPOS' signals. For example, MaxInputFrequency could only be guessed at and only with extensive monitoring of a mobile phone in different operating conditions. At best, Ingenico could determine a typical input frequency, but would have no way of knowing BBPOS' absolute maximum frequency in all operating conditions. In addition, Ingenico would have to monitor BBPOS' signals generated for all 442 mobile phones under different operating conditions to approximate the same information BBPOS accumulated over many months and years of their development and testing of mPOS devices. Utilizing the parameters and communications tabulated by BBPOS would have saved Ingenico significant amount of time either monitoring BBPOS operation of different mobile phones or performing their own testing of the communication parameters with the various mobile phones.

5.4.1 Patterson does not disclose BBPOS' trades secrets regarding communication settings

112. In ¶111 of his report, Dr. Shamos claims that the Patterson patent teaches how to identify communication settings in any number of mobile devices.

> *"It was known to determine a type of device from its electrical properties. Patterson et al. U.S. Patent Application Publication 2004/0081099 ("Patterson"), entitled, "Identification System and Method for Recognizing Any One of a Number of Different Types of Devices," was published on April 29, 2004. It discloses:*
>
> *An identification system and method for recognizing a device as one of a plurality of different types of devices connected to at least one terminal of an information handling system includes supplying a test signal to a device in a test mode;* ***measuring an electrical characteristic of the device in response to the test signal being applied to the device in the test mode; and matching a representation of the electrical characteristic of the device with representations of the electrical characteristics of the plurality of devices for recognizing the device connected to the terminal as one of the plurality of different devices.*** *Patterson, Abstract*

> *Identification of external devices and moreover internal reconfiguration to accommodate input from or output to external devices is even more critical with respect to smaller, portable devices such as cell phones and PDAs where often only one connection or jack can be provided to receive a plug. Patterson, [0005]"*

113. Patterson discloses a general and abstract method for measuring and identifying the characteristics of a device at a particular point in time and comparing those characteristics to characteristics of other devices. It does not disclose a method for identifying the communication parameters provided in BBPOS' trade secrets. For example, it could not be used to identify a recommended operating range of parameters such as min or max frequency. It also cannot determine parameters that are used for configuring internal operation of a device such as AudioSource since these are not detectable by observation.

114. Therefore, at best Patterson discloses guidelines for how to go about identifying a limited number of fixed characteristics of certain devices. The methods of Patterson could not be used to account for all of the communication parameters and recommended configuration settings of all the phone models established by BBPOS.

5.4.2 Dorsey does not disclose BBPOS' trades secrets regarding adaptive threshold or automatic gain control

115. In ¶114 of his report, Dr. Shamos claims that Dorsey discloses a method of adaptive thresholding:

> *"**The use of adaptive thresholding to process audio signal carrying digital data** was disclosed publicly in the above-referenced Dorsey application WO 2011/047042, specifically with respect to a credit card reader attached to a mobile phone.*
>
> …
>
> *115. Dorsey also discloses an adaptive threshold technique called "**reactive peak detection**":*

[0062] *Reactive peak detection is a heuristics based approach for peak detection, which is well suited for situations where the incoming signals from the card swipe is not excessively distorted by the mobile device's filter circuitry. This approach utilizes at least the following steps to detect signal peaks:*

*1. **Seed an adaptive positive and adaptive negative threshold** with an ambient noise value that is dependent on the hardware of the mobile device. These thresholds will be used for initial peak detection.*

2. Begin processing through the sample buffer, and for each sample in the buffer:

*3. **Wait for the threshold to be crossed** again when either the negative or positive threshold is crossed, except with a hysteresis factor applied to the threshold for the second crossing. The hysteresis factor is key in making this approach resistant to ringing in the incoming signals, which is associated with the active filter(s) of the platform hardware.*

*4. Begin looking for slope changes within this time frame once the two samples **where the threshold is crossed** have been established.*

116. This is not the same method of BBPOS' trade secrets for adaptive thresholding. Dr. Shamos omitted an important part of the Dorsey steps that differ from BBPOS' method. Dorsey's method continues in par. 0062:

5. If more than one slope change is found, compute the midpoint of the two samples.

6. If only a single slope change is detected, then

a. Pick the maximum point for the slope change.

b. Compare the peak's amplitude to the previously found peak's amplitude (if this has been established).

*c. Skip the current peak and move on if its amplitude is greater than (([full scale] - [current peak amplitude]) / ([full scale] *100) + 100) % of the previous peak's amplitude.*

7. If the prior step did not result in skipping of the peak, check the peak's polarity against the previous peak's polarity.

a. If the peak's polarity is the same as the previous peak's polarity, then remove the previous peak and put the current peak in its place.

b. If the polarity of the current peak has changed, then simply add the current peak to the list of peaks. This step is another key component for making this approach resistant to ringing.

8. Upon the finding of a peak, update the adaptive threshold of the corresponding polarity as the polarity of the peak just found and the amplitude to be a percentage of this peak's amplitude. Here, the percentage is a parameter varied by the detection approach being used, since higher values more accurately detects peaks, but are not as resistant to noise, while lower values are more resistant to noise, but may pick up errant peaks associated with ringing.

117. Steps 4 and 5 of Dorsey requires determining a slope change in sample peaks that have crossed the current threshold. This is not utilized in BBPOS' method.

118. Step 6 involves the skipping of a peak sample if they exceed a certain amplitude. This is not utilized in BBPOS' method.

119. Step 8 involves the calculation of a new threshold based on a percentage of the current peak's amplitude. This is very different from BBPOS' method of determining a new threshold based on a moving average of previous audio wave transitions (peaks).

120. Additionally, Dorsey does not disclose the specific types of pre and post filtering of the signals to both eliminate specific types of noise as well as "glitches" that occur in specific mobile phone models based on different communication speeds. [¶¶93-99 Expert Report of Ivan Zatkovich, dated February 16, 2022 in this matter]

121. Dorsey shows that the concept of adaptive thresholds may have existed prior to the development of BBPOS' specific method of implementing adaptive thresholds. However, Dorsey's method of adaptive threshold is different than BBPOS's method and therefore does not disclose the trade secrets.

5.5 Prior Art relating to BBPOS' proprietary mPOS communication formats and BBPOS' Data Security / Encryption Methods (data DUKPT method)

5.5.1 BBPOS' Proprietary communication formats were not publicly available

122. In ¶118 of his report, Dr. Shamos claims that the proprietary formats used in the BBPOS mPOS devices were publicly available.

> *"The formats used by payment applications were publicly available. In 2002, Bank of America published a large number of payment card formats in its "Bank of America Merchant Services MultiLink® Message Specification Authorization Formats for Debit, Credit, EBT, Check Acceptance and POS Check Version 4.02."*[6]

123. BBPOS designed proprietary formats for using their mPOS device with specific client card reader and payment applications. Some of these formats were of great interest to Ingenico as they were looking to sell their new devices to the same customers who had already developed these proprietary communication formats with BBPOS devices. BBPOS specifically designed formats 11 and 29 under NDA for their clients.

124. Some of the specifications for the communication formats were available publicly, and some would only have been available to registered and/or licensed developers approved to utilize those formats. However, BBPOS provided details in their descriptions of the 25 formats to Ingenico that were not necessarily present in the public domain or were were only available to registered/licensed developers. In fact, none of the 25 client specific formats designed by BBPOS were available publicly.

125. Lastly, some of the formats (e.g. Format 11 and 29) were defined by BBPOS that included their own proprietary formats and/or encryption methods which they only provided to their licensed users under non-disclosure. The only way for Ingenico to obtain these formats,

other than receiving them from BBPOS, was to obtain them from a customer who decides to break their NDA with BBPOS.

126. Ingenico chose to implement these formats for their devices for customers who were already using BBPOS formats 11 and 29.

5.5.2 Unitech did not publish BBPOS' Proprietary communication formats

127. In ¶119 of his report, Dr. Shamos claims Unitech published numerous formats for use with its own magnetic stripe card readers.

> *"In 2011, Unitech published a user manual[7] for its MS246 Magnetic Stripe Reader that listed numerous payment card and DUKPT formats. Thus, these were not trade secrets."*

128. Unitech's user manual, and many similar documents may describe the 'types' of information to be expected as credit card transaction data. However, it does not provide the proprietary message formats required by payment service providers such as PayPal, NAB, Google, PayPass, and Chase. And it certainly does not disclose proprietary formats defined by BBPOS such as formats 11 and 29. Similarly, the Unitech document may describe various ways of deriving keys for DUKPT related encryption, but it certainly does not disclose the specific methods BBPOS used to derive their Data DUKPT encryption method.

129. Therefore, Unitech's user manual would not satisfy the requirements of payment application providers who had BBPOS-developed communication formats specific to their needs.

5.5.3 BBPOS' Proprietary communication formats could not be obtained through reverse engineering

130. In ¶122 of his report, Dr. Shamos claims that simple reverse engineering methods could obtain the proprietary communication formats that BBPOS developed.

> *"Further, any mPOS communication formats used in any BBPOS product could be readily ascertained by reverse engineering simply by capturing communications between the product and a mobile device and examining their formats."*

I disagree with Dr. Shamos' characterization of "readily ascertained by reverse engineering" of the format specifications that would not have been legitimately available to Ingenico. Ascertaining even the simplest formats would have required some effort in determining the derived information in the communication as opposed to the fixed information coming directly from the credit card. The derived information comes from an internal process or algorithm in the mPOS device which can be very difficult to determine with any certainty. In addition, some of the derived information, especially the proprietary formats that BBPOS developed, could not have been reverse engineered by Ingenico without trade secret information from BBPOS. One such trade secret is the method for calculating BBPOS' Data DUKPT derived encryption in Formats 11 and 29.

131. This is because any data field that is encrypted, calculated, or derived in the software of the mPOS or SDK could not have been reverse engineered simply by sniffing the communications between the mPOS and the mobile phone (which for some of the formats is most of the data in the message). For example, some data fields could have been sniffed, but not sensitive data fields or enablement flags. Sensitive data fields would have been encrypted and thus not discernable if captured without a way to decrypt. In the case of enablement flags or mapped fields, these would not have been understood without some definition as to their meaning.

132. Therefore, signal sniffing without BBPOS confidential information regarding DUKPT decryption methods or communication formats, wherein enablement flags and mapped fields exist, would have been fruitless.

5.5.4 BBPOS' proprietary Data DUKPT algorithm was in use with BBPOS clients

133. In ¶126 of his report, Dr. Shamos claims that BBPOS data DUKPT method was disparaged by the payment industry:

> *"…. Furthermore, **I understand that this BBPOS variation on DUKPT was disparaged by the payment industry** and was rejected by Visa when Roam Data attempted to obtain Visa Ready Approval for it. Visa Ready was a security standard promulgated before PCI SSC released a PCI standard applicable to card readers without PIN entry capability." [emphasis added]*

134. I am not sure how accurate this characterization is, because BBPOS implemented this specific data DUKPT method for several of their customers in the industry. In addition, it did not prevent Ingenico from incorporating Formats 11 and 29, which included BBPOS' data DUKPT encryption method, into their device requirements. BBPOS used their Data DUKPT method in early implementations of their mPOS applications, for instance PayPal. As such, anyone building competitive devise and applications for these same customers would have benefitted from using the same formats and methods for seamless transition.

135. Therefore, regardless of what Dr. Shamos' opinion is regarding the industry's view of BBPOS' proprietary data DUKPT encryption methods, it was used in the industry by BBPOS' clients and Ingenico did incorporate this BBPOS trade secret into their product requirements.

5.5.5 BBPOS' proprietary Data DUKPT algorithm was an innovative design

136. In ¶¶127-128 of his report, Dr. Shamos claims that applying an algorithm already known in a different way is not a trade secret.

> *"127. What BBPOS actually did was to apply the DUKPT standard used for encrypting PINs and used it for encrypting non-PIN data. The algorithms were already known – **BBPOS just applied them in a nonconforming manner**.*
>
> *128. I understand from Mr. Rotsaert that Ingenico did not use this modification, except in a prototype for the Cartes demonstration." [emphasis added]*

137. Dr. Shamos is indicating that BBPOS' proprietary method of modifying the DUKPT encryption method does not conform to industry standards. This is essentially the perfect example of a trade secret. Ingenico's own product requirements, cited in my previous report at Sections 6.3.4 and 6.3.5, specifically indicate that Ingenico included BBPOS' proprietary Formats 11 and 29 into their product requirements. These formats require BBPOS' proprietary data DUKPT encryption method to produce specific data within those Formats.

5.5.6 BBPOS' proprietary encryption methods could not be easily reverse engineered

138. In ¶129 of his report, Dr. Shamos claims the BBPOS encryption methods and proprietary communication formats would have been easy to obtain through reverse engineering.

> *"129. To the extent that any encryption methods are embodied in any BBPOS product, they could be readily ascertained by reverse engineering the mobile phone code that performs decryption."*

139. This is not correct. By their very nature data encryption methods, such as BBPOS' Data DUKPT, are intended to be extremely difficult, if not highly improbable, to determine or reverse engineer.

140. In addition, Dr. Shamos, in ¶40 of his report, suggests that mPOS solutions were easily reverse engineered based on a paper entitled "Security Analysis of Smartphone Point-of-Sale Systems," by Frisby et al.

> *The mPOS market was much more advanced than Mr. Zatkovich suggests. A paper entitled "Security Analysis of Smartphone Point-of-Sale Systems," by Frisby et al. appeared in the proceedings of the Usenix Conference in August 2012. It contains a security analysis of multiple mPOS systems, including Square, Roam, IDTech UniMag II, and Verifone vx670. The paper is notable for the ease with which the authors were able to reverse-engineer these publicly available devices.*

141. I disagree this has any bearing on being able to reverse engineer any of the trade secrets that BBPOS included in their mPOS products. The Frisby Report is targeted at showing the vulnerabilities of mPOS devices. It does not disclose any of the BBPOS Trade Secrets. At best it describes the use of standard methods for DUKPT key derivation and recovery, and how to use some publicly available information to reverse engineer certain aspects of mobile phone applications. Note that BBPOS trade secrets regarding data DUKPT encryption was neither a standard encryption method nor was it made known publicly. The Frisby document does not describe how to determine or reverse engineer a specific method that was used to encrypt data nor any information present within the BBPOS trade secrets.

142. Ingenico would have needed to obtain the algorithms from BBPOS to include them in their mPOS products, which they did by receiving the actual algorithms and working with BBPOS engineers to test with their existing products (see Section 6.7 below).

143. Therefore, Ingenico had no reason to attempt to reverse engineer the BBPOS trade secrets for Data DUKPT and proprietary Communication Formats even if they could have been successful. Ingenico found these trade secrets useful and included them in their mPOS product designs.

6 BBPOS SHARED TRADE SECRETS WITH ROAM/INGENICO

6.1 Information Sharing Timeline and Relationship Activities

144. Dr. Shamos claims there are not sufficient indicators of confidentiality on documents shared.

> *138. As a threshold matter, I have examined all the BBPOS documents Mr. Zatkovich has alleged were provided to Roam containing supposed trade secrets. Only a handful of them contains any confidentiality notice (other than the word "CONFIDENTIAL" that was added belatedly during Bates numbering).*

145. Dr. Shamos is confused about when this type of designation is required. This is a matter of contractual commitment between vendor and customer. BBPOS has an agreement with their customer, ROAM. And because it was between ROAM and BBPOS only, sharing of information was open between these parties. MNDA agreements were in place in addition to the License agreement referenced in my original report.

6.2 BBPOS trade secrets shared with ROAM

146. Dr. Shamos shares that his discussion with Christopher Rotsaert indicates that Landi had mobile phone support in their products prior to 2012. However, he provides no information as to what kind of products are being supported (e.g. mPOS or other) and how the mobile phones are used with those products.

147. By March of 2012, Mr. Rotsaert made it clear that the mPOS product, that Landi was developing based on model S055, was still lacking certain capabilities and they were in need of assistance from BBPOS, specifically in the area of audio jack interface and power management.

> *Nevertheless,* ***this platform is quite new in Landi and not all features are yet available : in particular, swipe, audio jack interface & power management are not ready****. I'd like to discuss with you at Cartes & next week on how we could manage to move fast* ***leveraging both teams****. Liu Shying, R&D VP of Landi will be at Cartes on Wednesday & Thursday, I'd like to organize a discussion together on this opportunity. [email dated Mar 26, 2012 from C. Rotseart to Ben Lo - BBPOS_1682180-BBPOS_1682184, emphasis added]*

148. Note that this request comes after they had already announced that their mPOS product was targeted for release in 3Q12 as shown in the Management Review meetings between Ingenico and Landi for S055 audio interface product. [Page 34, IngenicoInc_0065410-IngenicoInc_0065456]

149. Later in May, 2012, Mr. Rotsaert is seeking additional information on BBPOS trade secrets which he will need in preparation for a workshop with the Ingenico R&D team (located in Valence). He also mentions that he wants to benchmark with an alternative solution from Ingenico.

> *Please do not forget to **send me all materials you have about swipe + EMV Chip product**.*
>
> > *Schematic,*
> > *Your selected core IC specification*
> > *Software synoptic,*
> > *Memory mapping estimation (information from Mobeewave : 256ko Flash & 100ko RAM for EMV contact et contactless)*
> > *Current status on the platform M-Core (what is already available / to be developed) availability of a development board with all targeted device functionalities >> what is already running on NFC-Swipe versus what remain to be done BOM breakdown estimation,*
> > *Battery capacity (likely to be smaller than with a ARM9 platform),*
>
> *...*
> *Based on a first discussion with Ingenico R&D director next week on Wednesday, I will confirm to you if we organize a **confcall or a workshop in Valence with your team**. As discussed during our call, I need to demonstrate that the project is really under control with visibility on our Time to Market. I want to avoid weeks of discussion whereas we shall release this device before end of the year with a **Press Release during Cartes Paris (6-8 November 2012)***
> *...*
> *As mentioned during our call, I need from you all package information you have on the swipe & chip device : schematic / functional architecture, EMV L2 certification report, development plan, schedule & budget **to be able to benchmark with alternative solution from ingenico**. [email string between C. Rotsaert and Ben Lo, May 15-18, 2012 - BBPOS_0000003-BBPOS_0000005, emphasis added]*

150. In July, 2012, Mr. Rotsaert then requested from BBPOS further information on the BBPOS designs for Audio interface, including polarity detection, power management, and the adaptive method for automatic gain control, as well as communication formats which include the Data DUKPT method.

151. The following email string excerpt shows a conversation between Mr. Rotsaert and BBPOS Engineer Daniel Tsai regarding the Power Management trade secret:

> *De : Daniel Tsai [mailto:danieltsai@bbpos.com.hk]*
> *Envoyé : vendredi 27 juillet 2012 11:59*
> *A: Christopher ROTSAERT*
> *Objet : Re: One missing scheme for explanation : solution to handle the 2 categories of phones for amplitude definition*
>
> *Hi Christopher,*
>
> *1)The power regeneration circuit and the coin cell are wired together via two diodes with very low forward voltage drop, that means the coin cell will compensate what was missing.*
>
> *2)The power consumption during waiting is lower than during reading card and calculating, so its higher chance that the phone can provide necessary power and coin only gives out a little or even no power during that period of time.*
>
> *3) Yes, it works even if the coin is not there.*
>
> *2012/7/21 Christopher ROTSAERT <Christopher ROTSAERT@ingenico.com>*
>
> *Daniel,*
> *Thanks.*
> *Just to confirm information:*
>
> - *Does the swiper pulls full power from coin under a certain (fixed ?) level of energy provided by the mobile or does the design enables to pull only necessary energy to compensate what was missing ?*
> - *In case of some Android phones providing low power, would the swiper use only power from mobile if the time before swiping is long enough ?*
> - *In case of iOS device (you mentioned that they deliver highest power level), the coin battery is not used ; meaning that lifetime on an iOS swiper is not limited by the coin. Correct ?*
>
> *[IngenicoInc_0048390-IngenicoInc_0048391]*

152. Another email string shows BBPOS engineer, Daniel Tsai sending documents Mr. Rotsaert requested for the Communication Format and the Audio Interface design, including

power management circuit. Copies of these documents had been sent earlier in the year but were requested again.

> *From: Daniel Tsai*
> *Sent: Monday, July 16, 2012 9:44 AM UTC*
> *To: Christopher ROTSAERTCC: Ben Lo*
> *Subject: The documents you requested*
> *[BBPOS_0005630]*
>
> *Attached Documents:*
> - *Phone list.xlsx [BBPOS_0005631]*
> - *BBPOS-DataOutputFormat-V1.15.doc [BBPOS_0005633-BBPOS_0005645]*
> - *audio interface.pdf [BBPOS_0005632]*

153. Several more documents are resent to Mr. Rotsaert at this time, including the Paypal Schematic which shows both the Polarity circuit and the Power Management circuit design, the EMV Flow, Two Communications, and Output Format v1.21 which also relies on use of the Data DUKPT method.

> *From:Daniel Tsai <danieltsai@bbpos.com.hk>*
> *To:ChristopherROTSAERT*
> *cc:Ben Lo*
> *Sent:7/16/20129:44:07AM*
> *Subject: The documents you requested*
> *[IngenicoInc_0009651]*
>
> *Attached Documents:*
> - *BBPOS EMVFlow.docx [IngenicoInc_0009626-IngenicoInc_0009627*
> - *BBPOS TwoWayCommunication.docx [IngenicoInc_0009628-IngenicoInc_0009629]*
> - *BBPOS-DataOutputFormat-V1.21.doc [IngenicoInc_0009636-IngenicoInc_0009650]*
> - *Paypal-PCB1-ST04-V3.1.pdf [IngenicoInc_0009622-IngenicoInc_0009624]*

154. Dr. Shamos indicates that ROAM never received information from BBPOS regarding the EMV and NFC capabilities.

> *151. In ¶ 128, Mr. Zatkovich says that "BBPOS began providing information to the ROAM Data team in Feb 2012 to continue development on the next*

> *version of EMV and NFC enhancements." It is true that Roam was working on EMV and NFC, but* ***there is no evidence that BBPOS provided Roam any disclosures relating to EMV or NFC****. [emphasis added]*

155. EMV is short for the Europay, Mastercard, Visa standard for "chip and pin" technology where you "dip", or insert, your credit card into a slot in the mPOS device to capture and send your credit card information, rather than a swipe operation or NFC operation. NFC refers to 'contactless' capability where you use your credit card to "tap and pay" or "hover" over the mPOS device to send your credit card information, rather than to insert or swipe your card. The audio jack interface between the mPOS device and the mobile phone would require essentially the same functionality regardless of whether the card was being read using a swipe, an EMV insert, or an NFC tap to pay.

156. Dr. Shamos' assertion is not correct. In February 2012, Mr. Rotsaert visits the BBPOS office and, in advance of his visit, makes this request via email. The request for information on chip (EMV) and "cless" (aka NFC contactless) readers indicates he is requesting information on their EMV and NFC developments.

> *In order to prepare this visit and as discussed, please find a list of topics I'd like to address :*
>
> *…*
>
> - *R&D development capability & equipments*
> - *Legacy portfolio of BBPOS in term of products, reference design, security (physical, logical), applications*
> - *Development activities by BBPOS for Roam Data in scope of readers (hardware, firmware), mobile application, gateway /servers, keys management*
> - *Introduction of BBPOS activities for other customers with relative dependences with activities for Roam Data*
>
> *…*
>
> - *R&D developments roadmap : hardware, firmware & security roadmap for swipe / swipe+Cless&* ***swipe+chip+Cless*** *readers*
> - *Product requirements documents introduction : features, performance, certifications*
> - *Actual schedule for new products developments*

- *Roam Data - BBPOS plans for **EMV contact/contactless** support (functionality & solutions in-house/outsourced)*
- *Keys management & Keys / Firmware loading process*

…

- *Scope of current / foreseen developments (wallet, RoamPay...), development model between Roam Data & BBPOS (ownership of sepc, developments...), relative agreement*
- *BBPOS roadmap, if applicable, in scope of software in mobile applications (IDE, SDK, API), server applications*

[BBPOS_0646802-BBPOS_0646804]

157. And on February 27, 2012, BBPOS sends two of their **NFC swipers** to Roam Data in Boston so that they can try with the Google RoamPay App. [BBPOS_0649030]

158. In addition, Dr. Shamos claims his support for BBPOS not sharing trade secret information is that Mr. Rotsaert continually complains that BBPOS is not providing the information being requested.

152. In ¶ 132, Mr. Zatkovich states that "Coupled with the assumption that an Acquisition of BBPOS was in process, the BBPOS team complies with all requests to provide information on their product designs and status." He cites no authority for that statement, and Mr. Rotsaert informs me that he complained numerous times to BBPOS that he was not getting the requested information.

159. It appears that Mr. Rotsaert is the only resource Dr. Shamos is relying upon for this information which is conclusory at best.

160. Clearly, Mr. Rotsaert is receiving information about both the EMV and NFC capabilities that BBPOS has developed. Mr. Rotsaert actively engages in dialog regarding these designs with the BBPOS engineers as shown in emails such as the one from May 23, 2012:

FOR NFC PROJECT:

- For the NFC PCB we may need extra few days till 15th June, as I forgot to take into account that we need to add power circuits to our board for supplying the RF amplifier.

- Now the L1 protocol stack is running inside the PN533, and for all upper level functions will use RAM and FLASH in host MCU. In case lack of memory resources, we can use a compatible MCU with more internal memory in the same family.

FOR EMV PROJECT:

- I have attached the schematic diagram, datasheet of the MO MCU now using, datasheet of the EMV controller IC which has built-in, and datasheet of the M4 MCUI suggested.

- We haven't start the porting of contact L2 to cortex M core platform, but I believe it can be fitted into the ST Cortex M4 platform I chooses.

- The currently developed code in cortex MO which can be ported into M4 are: Audio communication, Magnetic head decoding, USB generic HID, key management, encryption, bootloader.

[IngenicoInc_0010296-IngenicoInc_0010306]

161. In response to BBPOS, Mr. Rotsaert provides a thank you message and posts these additional questions regarding the design.

Thanks for the information.

1) Swipe —-NFC
Didn't you implement already some commands for Google usecase on the MO?

2) Swipe — Chip EMV
Do you have a preliminary BOMfor the Swipe EMV Chip ? Could you please give me prices (even estimated) for the key components you listed.

Regarding battery, what is your assumption for capacity ? 200mA ? more/less?

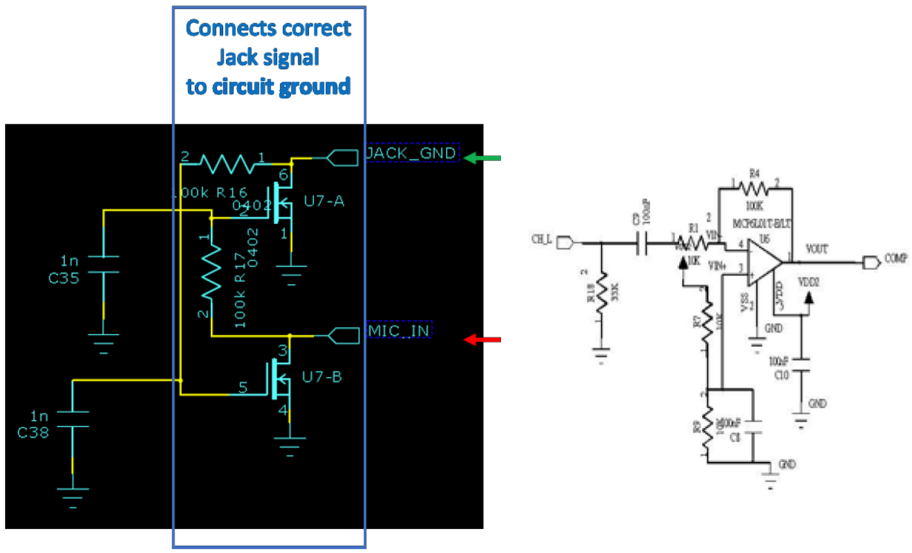
What is current memory size you use for functions you listed : Audio communication, Magnetic head decoding, USB generic HID, key management, encryption, bootloader.

[IngenicoInc_0010296-IngenicoInc_0010306, emphasis added]

6.3 Audio Jack Polarity Detection trade secret information requested/received

162. In his report, Dr. Shamos claims that circuit below on the left is not the same as the circuit below on the right.

> *156. Further, it is not even clear what the "polarity detection circuit" consists of. The circuit diagram illustrated in ¶ 70 of the Zatkovich Report is different from the circuit he says in ¶ 141 is the polarity detection circuit. The ¶ 70 circuit is shown on the left below. The ¶ 141 circuit is on the right.*

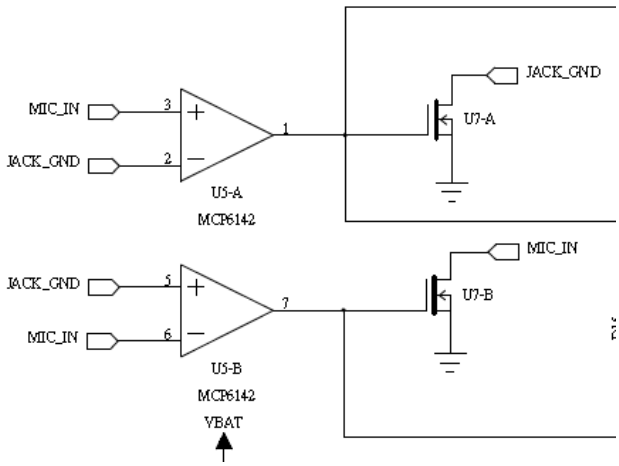


BBPOS Polarity Detection circuit

> *157. These circuits are not the same. They differ in the number and arrangement of components.*

163. However, Dr. Shamos is comparing the wrong circuits. The circuit on the left above is one version of the polarity detection circuit that BBPOS shared with Roam and Ingenico. Another schematic [BBPOS_0005665], that I reference in both ¶140 and ¶141 in my previous report, contains both a polarity detection circuit and a power management circuit. All versions of polarity detection circuits that BBPOS designed must accept JACKGND and MICIN signals as input, since these are the two signals that must compared in order to determine and correct the

polarity. These two signals are shown in the circuit above on the left as well in the schematic [BBPOS_0005665] below.



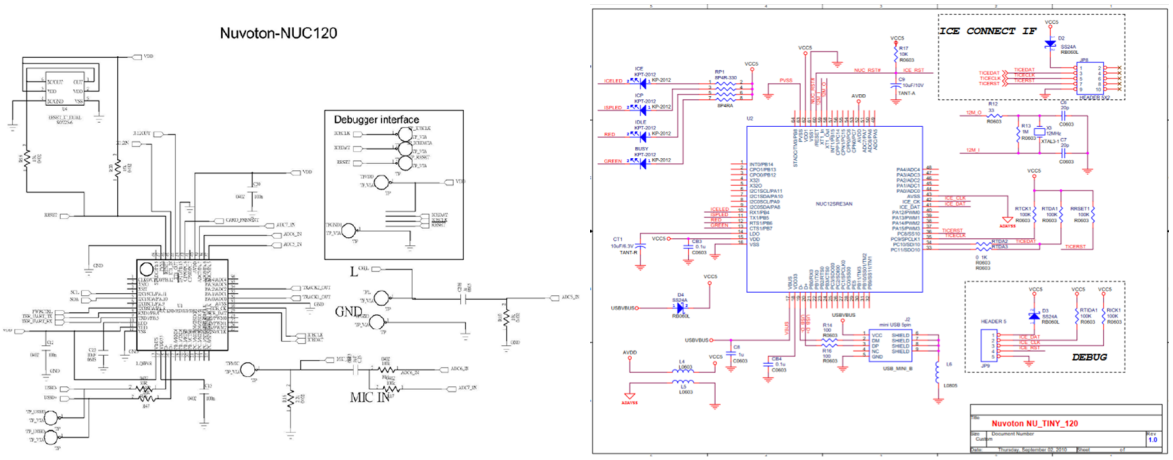
[BBPOS_0005665]

164. Dr. Shamos, however, is comparing a BBPOS polarity detection circuit with a BBPOS power management circuit. In all cases the BBPOS polarity detection circuits are well defined because of use of the JACKGND / MICIN signals and the fact that Ingenico correctly incorporated this design in their RP350X, RP750X, RP100 series, and RP450 series products.

6.4 Power Management trade secret information requested/received

165. Dr. Shamos claims the schematics shared are for third party data sheets when in fact there were also schematics for the EMVSwiper as well.

> *159. In ¶ 141, Mr. Zatkovich refers to disclosure of schematics allegedly sent from BBPOS to Roam. These schematics are misleading because they consist primarily of drawings taken from chip manufacturers' data sheets, and, to that extent, they were not created by BBPOS. For example, Mr. Zatkovich points to IngenicoInc_0010195-200, but this contains a data sheet from Nuvoton, whose NUC120 chip was proposed to be used. At left below is IngenicoInc_0010195. At right is a NUC120 data sheet I obtained from https://media.digikey.com/pdf/Data%20Sheets/Nuvoton%20PDFs/NUC120.pdf*



160. Mr. Zatkovich does not identify what portion, if any, of the shared documents represents the alleged trade secrets and which portions are simply reproduced from third-party sources. A third-party data sheet is not a trade secret of BBPOS. None of the schematics bears any confidentiality markings.

166. In ¶141 of my previous report, I refer to an email string [IngenicoInc_0010195-IngenicoInc_0010200] which consists of an email between BBPOS engineers and Mr. Rotsaert describing the characteristics of a complete electronics design of the EMV_Swiper which includes third party chips as well as their proprietary circuitry for power management. The text in ¶141 of my previous report actually indicates there are Attachments consisting of: 3 datasheets for chips being used by BBPOS in their design along with a schematic showing the EMV Swiper electronics design. The EMV Swiper schematic is comprised of 6 pages of electronic design schematics, some of them identifying third-party chipsets as would be necessary in any circuit schematics. The bulk of the information in these documents, most pertinent to Roam and Ingenico, were the proprietary BBPOS designs for the mPOS functionality. In addition, the schematics are also marked as to which pages are third-party chips vs EMVSwiper functions.

6.5 Automatic Gain Control (and SDK) trade secret information requested/received

167. Dr. Shamos claims none of the alleged communication parameters were shared with Roam in the cited references.

> *161. In ¶ 142, Mr. Zatkovich points to two documents allegedly containing disclosures of this trade secret, IngenicoInc_0009756-9767 and IngenicoInc_0283863-864. These documents together constitute only four pages, without any confidentiality markings, and no circuit diagrams. However, in ¶¶ 91-92, Mr. Zatkovich refers to 11 parameters BBPOS measured for 442 mobile phone models, i.e., 4862 parameters. The four pages disclosed to Roam do not contain even a single one of those parameters, and Mr. Zatkovich presents no evidence that either the 11 types of parameters, or any individual value of any parameter for any particular mobile phone model was ever disclosed to Roam.*

168. The references he cited refer to conversations between the BBPOS engineers, ROAM Data and Ingenico regarding the SDK releases which would include the parameters to accommodate for the different phone models as addressed in my previous report.

169. However, Dr. Shamos neglects the fact BBPOS shared their SDK software with ROAM and Ingenico on multiple occasions as updates were made and testing was performed between the two teams. The SDK software contains the code for communication parameters, auto gain control / adaptive threshold, and the communication formats. This email shows the SDK code is shared from BBPOS Engineer, Jimmy Tang, to Roam Data Engineer, Eran Hollander.

> *From: Jimmy Tang*
> *Sent: Monday, July 9, 2012 3:02 PM UTC*
> *To: Eran Hollander; Jimmy Tang*
> *Subject: iOS and Android SDK*
> *Attachments:* ***RoamPayApi 4.0.0 iOS SDK v1.0.zyp, RoamPayApi 4.0.0 Android SDK v1.0.zyp***
>
> *Hi Eran,*
>
> *Please find enclosed two SDK files. Need to rename to .zip.*
>
> *Regards, Jimmy*
>
> *[BBPOS_0651362 emphasis added]*

170. The email below shows the discussion between the BBPOS team, Roam Data team and Mr. Rotsaert of Ingenico regarding the testing of the BBPOS SDKs.

From: John Chiu

Sent: Monday, May 7, 2012 2:45 PM UTC
To: Eran Hollander; Christopher ROTSAERT; Jimmy Tang; Bill Bachrach; Will Graylin; Stuart Fullerton
Subject: iOS issue discovered in testing

Hi,

We discovered an iOS issue in testing late on Friday. After speaking with Eran today, it was agreed as a blocking issue. We can turn this around quickly, but it will delay iOS SDK availability by 2-3 days. We are working with the HK team to get the issue resolved. We do not have release schedule yet,

I will keep everyone advised on the status and new release date.

Best, John

[BBPOS_0004844]

171. The following email is informational about the next BBPOS SDK release and the project plan associated. This is shared between the BBPOS team, Roam Data team and Mr. Rotsaert of Ingenico.

From: Eran Hollander
Sent: Saturday, May 19, 2012 2:11 AM UTC
To: Michael Arner; John Chiu; Jimmy Tang; Ebon Kim; Bill Bachrach; Will Graylin; Christopher Rotsaert; Christopher Miller; Richie Sun; John Coloe; Anthony Davis
Subject: Project 4.0 project plan
Attachments: RoamPay API PPLAN 5-18.pdf

All,

Here is the pplan for the SDK 4.0 and imobile app 4.0. Overall seems like both projects will end sep 6th. However, I believe this is optimistic and doesn't leave any room for error….

*[*BBPOS_1633041*]*

6.6 Communication Formats (and SDK) trade secret information requested/received

172. Dr. Shamos claims a communication format is not a trade secret.

> *163. In ¶ 143, Mr. Zatkovich lists multiple documents relating to data formats that were disclosed to Roam. However, as I have already explained in ¶¶ 117-124, a communication format cannot be a trade secret because it is readily ascertainable by examining the communications themselves.*

173. In ¶¶91-95 above, I have addressed Dr. Shamos assertions that Communication Formats were publicly available and thus not a trade secret of BBPOS. They are in fact trade secrets because they are a proprietary method for communicating between the BBPOS devices and a specific payment vendor(s). The communication formats include encrypted fields, enablement flags and fields mapped to proprietary data; none of which was made publicly available by BBPOS.

174. In ¶120 of Dr. Shamos report, he claims that the payment vendors design the communication formats.

> *120. In ¶ 100, Mr. Zatkovich refers to "BBPOS' proprietary mPOS communication formats." However, the formats simply arrange information that is required to be communicated to a specific vendor's (e.g. PayPal's) payment application. The required information is specified by the payment application provider, not by BBPOS.*

175. This is an inaccurate characterization. The various communication formats have some data fields that are similar and some data fields that are different, and many data fields that are encrypted in different ways. In all cases the formats are proprietary to either BBPOS or the different vendors and are not publicly available.

176. And in ¶122 of his report, Dr. Shamos, claims that these proprietary Communication Formats could be easily ascertained through reverse engineering.

> *122. Further, any mPOS communication formats used in any BBPOS product could be readily ascertained by reverse engineering simply by capturing communications between the product and a mobile device and examining their formats.*

177. As stated above, in ¶¶99-101, I address this assertion based on the BBPOS' proprietary Communication Formats having encrypted data, derived or calculated data, such as enablement flags for example. The contents of these data fields can only be determined with Field specifications such as BBPOS' communication format documentation, or access to BBPOS' SDK code.

178. Then in ¶123 of Dr. Shamos report, he claims he cannot understand from my report the business advantage to BBPOS of having these trade secrets.

> *123. Mr. Zatkovich does not explain what business advantage any of the formats provided to BBPOS, which I understand is a requirement for a trade secret.*

179. These trade secrets provided business advantage to BBPOS through the ability to continue working with existing customers like Paypal and Google to implement newer advanced technologies such as EMV and NFC products. Having these formats in place allowed a quicker time to market for these new products for these payment vendors and guaranteed a more stable warranty period as the testing of the information exchange had already completed. In addition, there is an advantage of having multiple communication formats defined in a single SDK that supports many different vendors which again allows an easier introduction of new functionality and reduces the testing and integration time for the supported vendors using these proprietary formats.

180. This is precisely the type of leverage Ingenico was interested in because their mPOS product was lagging forecasted delivery dates and they were eager to switch customer over to their platform. Using the BBPOS proprietary, and tested, Communication Formats enabled them a quicker more stable deployment of their new mPOS functionality with these clients.

181. Dr. Shamos then claims there is no evidence that SwiperDecoder.java was disclosed to Ingenico which is used by BBPOS to understand the Communications Formats, and thus data, being received from the Swiper device.

> *124. In ¶ 106, Mr. Zatkovich displays some code from SwiperDecoder.java that supposedly interprets a format, but there is no evidence this code was ever disclosed to Ingenico. Further, the code is trivial, consisting of instructions to pluck various data fields out of a record. Any program written to perform the same function would necessarily resemble this code.*

182. As described above there is nothing trivial about determining derived or encrypted fields without documentation of those communication formats. SwiperDecoder.java is an example of code that code be used to interpret these Communication Formats. BBPOS provided documentation of Communication Formats to Ingenico on various occasions as new formats were created. Having this documentation enabled Ingenico to create code to interpret these formats.

- BBPOS Engineer, Daniel Tsai, provided BBPOS-DataOutputFormat-V1.15.doc on July 16, 2012 to Christopher Rotsaert. [BBPOS_0005649-BBPOS_0005663]
- BBPOS Engineer, Daniel Tsai, provided BBPOS-DataOutputFormat-V1.21.doc on July 17, 2012 to Christopjer Rotsaert. [BBPOS_0005649-BBPOS_0005663]

6.7 Data Security / DUKPT Data Encryption Methods trade secret information requested/received

183. Dr. Shamos claims the Data DUKPT method was not a trade secret.

> *164. In ¶ 144, Mr. Zatkovich lists various documents containing DUKPT source code that were sent to Roam. However DUKPT is a publicly available algorithm for which many open source code sets are available online. The only*

conceivable trade secret in BBPOS' DUKPT implementation, based on Mr. Zatkovich's description of the alleged trade secrets would be the non-standard variations introduced by BBPOS. Mr. Zatkovich does not indicate which, if any, portions of the code relate to the supposed trade secret.

184. The use of a standard DUKPT method for deriving an encryption key would not be considered a trade secret. However, BBPOS developed a non-standard DUKPT method for deriving an encryption key, which Dr. Shamos himself refers to as being "applied in a non-conforming manner." This BBPOS proprietary method is also evidenced in emails between Mr. Jerome Grandemenge from Ingenico and BBPOS' Jimmy Tang beginning on February 16, 2012, first with the transfer of the DUKPT code to Ingenico along with Communication Format 10 and continuing through iterations of testing until the Ingenico team has it working.

>> Hi,
>>
>> Attached is the codes for DUKPT algorithm in C++ and also the document about format 10.
>>
>> Jimmy
[BBPOS_0004382]

185. And then in reply, on February 20, 2012, is a string of emails including the one below between BBPOS Engineer, Jimmy Tang, and Ingenico Engineer, Jerome Grandemenge, regarding the implementation of the DUKPT method for integrating with the Ingenico devices.

From: Jerome GRANDEMENGE
Sent: Monday, February 20, 2012 9:42 AM UTC
To: Jimmy Tang
CC: Christopher ROTSAERT; derekchan@bbpos.com.hk; Ben Lo
Subject: RE: iWL - android with Roam Data solution

Hi Jimmy,

I did some good progress on the demo (using an iWL wireless terminal instead of the iST) and I should be able to send you some documentation today. How do you want to proceed then ? I understand you will need to integrate the iWL interface to the RoamPay API, right ?

At the moment, Roam encryption is not integrated in the demo but I integrated the code you provided me in a separate app and it seems to work, I get the same results on the iWL and on the PC which is a good news. I will soon integrate the encryption into but I need to perform more testing before doing that.

How should we proceed then ? Should I send you an iWL so you can start integrating it with the tablet ? On your side, it would be good also if you can provide me with a test account so I can also start playing with the roam player and the roam pay API.

Best regards / Cordialement,
Jérôme Grandemenge
[BBPOS_0004428-BBPOS_0004430]

186. These emails clearly show that BBPOS provided their DUKPT algorithm, in C++ code, to the Ingenico engineers and then further assisted with troubleshooting the integration to ensure they learn how to integrate with the Ingenico existing platforms. This information was both requested by Ingenico, received, and integrated.

7 ROAM/INGENICO'S USE OF THE TRADE SECRETS

7.1 Ingenico's use of BBPOS' Audio Jack Polarity Detection design

187. While Dr. Shamos opines about what was, or wasn't, known in the industry with regard to the opinions presented in my previous report, he confuses the fact of there being only two possible polarities with the actual trade secret that BBPOS shared with Ingenico. I agree, having only two possible polarities was definitely well known in the industry. However, the polarity detection and correction circuit designed by BBPOS was not.

188. Dr. Shamos provides the following references to my report to support his assertion.

167. In ¶ 149, Mr. Zatkovich cites a requirement document containing the requirement to "detect polarity to switch automatically MIS/GND." However, as I pointed out earlier, there are only two possible polarities, and switching to the correct polarity is essential for proper functioning of a device. It was not a trade secret. On the contrary, it was commonly known in the trade.

168. The fundamental problem with Mr. Zatkovich's demonstration is apparent in ¶¶ 152-153 and again in ¶¶ 154-155. In ¶¶ 152-153, Mr. Zatkovich reasons from the fact that both BBPOS and Ingenico circuits use two MOSFET transistors. However he fails to explain the fact that the BBPOS circuit uses two resistors (R16 and R17) and two capacitors (C38 and C35), while these four components are completely absent from the Ingenico circuit. Not only are these not the same circuit, but neither is derived from the other.

169. The photograph in ¶ 154 shows no more than that the Ingenico device has an audio jack attached to a circuit board. That is not a trade secret of BBPOS.

170. In ¶¶ 155, 157 and 160, Mr. Zatkovich says that the pairs of illustrated devices "use the same design," but they plainly do not.

171. In ¶¶ 156-159, Mr. Zatkovich compounds the problem by relying on photographs of Ingenico and BBPOS devices that look visually similar. However, an electrical engineer would know that comparison of circuits, not photographs, is what matters. All mPOS devices that connect to an audio jack have an audio plug. All polarity detection and correction circuits have a ground connection. A comparison of photographs is meaningless in this context.

189. In his statements, Dr. Shamos, seems to equate the trade secret with simply the use of two transistors, two resistors, and two capacitors and nothing else. It is clear that Dr. Shamos does not have a complete understanding of the operation of BBPOS' polarity detection and correction circuit. First, the two resistors and two capacitors in the BBPOS design have nothing to do with the actual function of detecting and correcting the polarity of the audio signal. Second, the primary value of BBPOS' design was that they were able to both detect and correct the polarity of the audio signal by utilizing two inexpensive transistors configured in a very simple and elegant way. As indicated in my previous report, BBPOS modified their design several times before they determined the most efficient version of that circuit that would still meet all the requirements of both detecting the polarity and automatically correcting the audio signal.

190. The basis of BBPOS' trade secret is first in the use of the MIC IN and Jack Ground signals as the detection means, by respectively applying each signal to the base or gate of the

transistor pair. Second, the opposite of those signals are then applied to the respective gated or switched input on each transistor so that one of the transistors would produce the corrected audio signal as the output. This is exactly the solution that Ingenico utilized in their product.

191. The fact that Ingenico directly relied on BBPOS' trade secret design is made even more evident from the fact that none of the prior art cited by Dr. Shamos discloses or even hints at this extremely efficient solution to the problem. The closest piece of prior art that provides any specificity on a circuitry design is the use of Texas Instruments specialty chip. As mentioned above, there is no disclosure within the chip design at all as to how it actually detects the polarity or corrects the audio signal other than the use of the descriptor "control logic".

192. In addition, the Texas Instruments chip costs approximately $0.35 in volume, whereas BBPOS' solution costs approximately $.01 - $.02 per transistor in volume. This is roughly 8 to 15 times the cost savings over the use of Dr. Shamos' closest identified prior art.

193. Regarding Dr. Shamos' assertion that my analysis relies merely on photographs with visual similarity is simply incorrect. My analysis was based on the fact that Ingenico's own circuit design drawings (shown in my previous report) showed that they used the same configuration of MIC IN and Jack Ground signals applied to the same base and input switched signals on the transistors.

194. This was further confirmed by my electrical testing of the accused transistor pairs. As a result of this electrical testing, I identified the location of the transistor pairs, as well as verifying the electrical configuration of the transistor used the same design as the BBPOS trade secrets.

195. Specifically, the source of the signals for the MIC IN and Jack Ground are identified in the first photo of each product tested (showing the location of the audio jack). And then the

location of the termination of those same signals is identified in the second photograph with the highlighted transistor pair. I then verified, electrically, that the MIC IN and Jack Ground were configured in these circuits in the exact same configuration, at the respective base and switched output, for the transistor pair as designed by BBPOS.

196. Knowing the specific circuit design, and the placement of the transistor pair that I identify in my report, Dr. Shamos could have performed this electrical test himself to confirm my analysis. Additionally, he could have simply asked Ingenico if this was in fact the way they designed their polarity detection circuit. Either way, this would have confirmed the analysis in my previous report.

7.2 Ingenico's use of BBPOS' Power Management design (Auto Power On)

197. Dr. Shamos claims that Ingenico did not use the BBPOS Power Management design when in fact they did incorporate it in the Ingenico RP350X, RP750X, the RP100 series, and the RP450 series.

> *172. In ¶¶ 160-167, Mr. Zatkovich says that Ingenico used BBPOS' "power management design." It did not. There is a profound difference between implementing a common feature and using a trade secret design in doing so. Mr. Zatkovich shows no more than that Ingenico implemented the feature.*
>
> *173. Mr. Zatkovich's allegations in ¶¶ 161-167 border on the ludicrous. He argues that it was a BBPOS trade secret to have a device turn on when it is plugged in. However, such a function is essential for a device that does not have an on/off switch, or there would be no way to render it operational.*
>
> *174. He does not exhibit any BBPOS circuit, yet somehow claims that Ingenico's circuits are "similar" to the undisclosed BBPOS circuit.*
>
> *175. In ¶ 167, Mr. Zatkovich says he tested various Ingenico devices and verified that "when that mPOS initialization occurs, the Ingenico device turns-on and remains on, exhibiting the same behavior as the BBPOS." However, the "behavior" is not a trade secret, even if a specific circuit to perform that behavior might be. However, Mr. Zatkovich does not show any BBPOS circuit to which an Ingenico device might be compared.*

> *176. The "behavior" to which Mr. Zatkovich refers was publicly available. BBPOS itself made this information in Chan, referred to above. It discloses:*
>
> *In general, in one aspect the invention provides a power management circuitry that is used in a peripheral electronic device. The power management circuitry includes a power regeneration circuitry, a power selector, a power switch and an audio signal detection circuitry. The power regeneration circuitry is configured to receive a continuous periodic sound wave from an audio device and to convert the continuous periodic sound wave into an amplified DC electrical signal. The power source selector is configured to receive a first input comprising the amplified DC electrical signal from the power regeneration circuitry and a second input from a primary power source and to provide a power signal output. The audio signal detection circuitry is configured to receive the amplified DC electrical signal from the power regeneration circuitry 52 and to transmit a wake-up signal to the power switch circuitry.* ***The power switch circuitry is configured to be turned on by the wake-up signal and to connect the power source selector to the peripheral electronic device main circuitry and thereby to transfer the power signal output to the peripheral electronic device main circuitry****. '001 Application, [0007]*

198. In ¶¶172 – 174 of Dr. Shamos' report, he asserts that my analysis amounts to simply the identification of a "common feature" along with an indication that the device turns on when plugged in. This of course, ignores the totality of my description of BBPOS' Power Management Trade secret (Zatkovich ¶¶77-83). This included an analysis of BBPOS' schematic containing 3 specific subcircuits. I labeled these subcircuits as the "temporary trigger" circuit, the "power switch" circuit, and the "permanent trigger" circuit.

199. I also describe the function and objective of each of these subcircuits, as well showing another BBPOS circuit schematic with an alternative version of that same solution with slight alternate versions of those 3 subcircuits. I then compare the design and operation of BBPOS' 3 subcircuits with a schematic of Ingenico's RP350X mPOS device. I identify the 3 subcircuits within Ingenico's schematic, and describe how each of those subcircuits have the exact function and objective as their BBPOS' counterpart subcircuits.

200. In addition, at ¶175 of Dr. Shamos' report, he reduces my analysis of the circuit behavior to that of "when that mPOS initialization occurs, the Ingenico device turns-on and remains on". This is clearly a drastic over-simplification. This portion of BBPOS' trade secret for Power Management requires that when the device is "temporarily" woken up by activity on the audio jack, the microprocess must analyze the incoming audio signals to determine if it matches the specific protocol of an mPOS device request or a card transaction request.

201. To do this, I tested the behavior of the Ingenico device, by applying various signals to the audio jack (monitored the device with an oscilloscope) to see if, and when, the device would wake up and stay awake. Only in the cases where I transmitted a valid mPOS command or card transaction request did the device wake up and stay awake. With all other test signals including music, the device would only wake up temporarily and then immediately go back to sleep. This is not just some similar general behavior; it is the exact behavior defined in the BBPOS trade secret.

202. Lastly, Dr. Shamos indicates that the Chan prior art discloses this same trade secret. As I have described above, Chan does not disclose the same BBPOS trade secret that defines 3 specific subcircuits (in schematic detail), and the verification of the incoming audio signals during the temporary wake up. All that Chan patent discloses is the high level function of a "***wake-up signal and to connect the power source selector to the peripheral electronic device main circuitry".*** There are no circuit schematics, no mention or even an indication of the 3 subcircuits, or the logic of verifying the incoming audio signal as a valid mPOS command.

203. The fact that Ingenico utilized both the 3 subcircuits having the exact same function and objective as BBPOS' design, as well as the verification of the audio signal during the temporary wakeup, indicates that Ingenico clearly utilized BBPOS' trade secret when developing

their products. This is made even more evident by the fact that Dr. Shamos could not identify any prior art that mentions or suggests a design with this type of 3 subcircuits, nor mentions the verification of data encoded on the audio signal during the temporary wake up period.

7.3 Ingenico's use of BBPOS' Pre-analyzed communication settings and adaptive threshold (or Auto Gain Control)

204. Dr. Shamos indicates that decompiling APIs from an SDK would produce the necessary information to implement this trade secret. However, while that is true for the Roam/Ingenico SDK, it is not true for the BBPOS SDK because BBPOS purposefully obfuscated their SDK object code to protect this information.

> *177. In ¶¶ 168-173, Mr. Zatkovich attempts to show that Ingenico used BBPOS' pre-analyzed communication settings and adaptive threshold. However, I showed above in ¶¶ 161-162 that the settings nor the adaptive threshold process was disclosed to Roam. Therefore, use, by Ingenico, if it occurred at all, could only have resulted from legitimate reverse engineering. Mr. Zatkovich himself says in ¶¶ 171-172 that he was able to reverse-engineer the settings from a SDK by decompiling APIs. Any information that can be obtained in this manner cannot be a trade secret.*

205. Dr. Shamos asserts that Ingenico's use of this BBPOS trade secret "if it occurred at all, could only have resulted from legitimate reverse engineering". This apparently relies on the assumption that I, as stated in my report, was able to reverse-engineer the [Ingenico] settings from the SDK by decompiling APIs. Dr. Shamos assumes that Ingenico could have done the same with BBPOS' SDK object code.

206. This is an incorrect assumption. I was only able to analyze Ingenico's SDK code because it was not "obfuscated". In other words, it was possible for me to recreate and analyze Ingenico's source code and data settings because they did not attempt to hide it in, or prevent decompilation of, their SDK object code.

207. However, all of BBPOS' object code within the SDK was heavily obfuscated to the point that it is not possible to identify any BBPOS code functions or data settings. In other words, it is only possible to reverse engineer Ingenico's object code but would not be possible to do the same with BBPOS' object code. The only reason I was able to analyze BBPOS' source code and communication settings was because BBPOS directly provided me with copies of their source code and associated data settings, which I analyzed and reproduced in my previous report.

7.4 Ingenico's use of BBPOS' BBPOS' Communication Formats

208. Dr. Shamos continues to claim that these formats were publicly available when they were not provided publicly by BBPOS or any vendors that developed communication formation. BBPOS also did not provided their proprietary formats to customer developers unless under NDA as shown in my previous report.

> *178. In ¶¶ 174-175, Mr. Zatkovich relies on a statement in a requirements document allegedly showing that Ingenico specified the use of BBPOS formats 11 and 29. There is no evidence that these requirements were ever implemented. In any case, the formats themselves were readily ascertainable simply by examining communications between an mPOS reader and a mobile phone and thus cannot be trade secrets.*

209. As I have indicated above, Ingenico could not have readily ascertained the communication formats since those details were not available to the public. A number of those formats would have been available only to registered/licensed developers that are implementing specific formats for specific vendors. In addition, for most of those formats, BBPOS was only able to define and document them after extensive testing and/or working with the vendors. And lastly, several of the communication formats were proprietary to BBPOS and not available elsewhere without a non-disclosure agreement.

7.5 Ingenico's use of BBPOS Data Security / Encryption Methods (DUKPT data method)

210. Dr. Shamos claims there is no proof that the Data DUKPT method was implemented by Ingenico/Landi.

> *179. In ¶¶ 176-179, Mr. Zatkovich points to three paragraphs of requirements documents specifying that "BBPOS encryption" should be used. There is no evidence, however, that any product was ever built satisfying that requirement, and Mr. Zatkovich's experiments with Ingenico products did not reveal any use of the "Data DUKPT" method developed by BBPOS.*
>
> *180. In ¶ 177, Mr. Zatkovich says that "Ingenico utilized this information in their product designs," but he cites no evidence in support except three sentences in requirements documents.*

211. Ingenico did utilize BBPOS' Data DUKPT trade secrets in their product designs. The product requirements document identifies the specific design features, including the BBPOS Data DUKPT design, that would be incorporated into their products. Dr. Shamos asserts that I provide no evidence "that any product was ever built satisfying that requirement, and Mr. Zatkovich's experiments with Ingenico products did not reveal any use of the 'Data DUKPT' method". However, Dr. Shamos should be aware that it would not be possible, or highly improbably to identify the use of a particular DUKPT encryption key derivation method within a working product. The whole intent of this and other encryption schemes is to prevent the key, or the key derivation method, from being discovered. Otherwise, the encryption method would be useless. Therefore, the requirements and design documents for Ingenico's next generation mPOS products, provide sufficient evidence that BBPOS' proprietary Data DUKPT method was intended for development and deployment in devices to be built by Landi.

8 VALUE OF BBPOS TRADE SECRETS

212. Based on Ingenico's IP expert's conclusions and discussions with Mr. Rotsaert at ¶74(a) – (e), the damages expert opines that BBPOS' trade secrets were of little or no value.

However, this is certainly not the case, otherwise Ingenico would have developed them internally or would not have included the features at all.

> *"offer little value to Ingenico's accused products, if any at all," and present zero damages, to the extent that the trade secrets could be ascertained via "independent invention, reverse engineering, or obtaining them through publicly available information." [Vanderhart ¶75]*

213. All of these trade secrets came about because of BBPOS experience and numerous trials in applying the technology. The only experience Ingenico had was how to process a card swipe in a non-mPOS mode. The trade secrets that Ingenico sought, and BBPOS provided, are all technical areas that would not have been encountered in Ingenico's prior experience and models. And without this information, Ingenico would have had to spend significant development and testing time to accomplish the same result. Specifically:

1) polarity detection, which is only necessary to interface an mPOS device with a mobile phone using an audio jack interface.
2) power management, which was needed to support the low power, transportable, small format of an mPOS device in order to keep it from having to be plugged into a power source for long periods of time in a retail environment, which would defeat the purpose of having a mobile device.
3) auto gain control, which is only required when interfacing an mPOS with an audio jack of a mobile phone. In fact, the primary reason BBPOS to develop auto gain control capability is that dozens of different manufacturers have different characteristics for different models of mobile phones thus necessitating an adaptive threshold and different communication parameters for each phone model.

4) Communication formats developed specifically for communication between mPOS and mobile phones; and are not used for any non-mPOS type device.

5) Data DUKPT method, developed specifically by BBPOS for their mPOS devices in order to create a more secure transfer of data.

214. Only a person familiar with the design and consumer requirements of these types of devices would be able to opine on the value provided by the accused products.

215. ROAM and Ingenico specifically, and repeatedly, requested these trade secrets from the BBPOS engineers because they saw the value of having these features without having to spend years of designing and testing, as BBPOS did, to develop these new capabilities specific to mPOS devices.

216. Mr. Rotsaert actually indicated several months before having to release a Landi product, that Landi did not have these important features yet. He requested time from Ben Lo of BBPOS to meet with he and Landi in Cartes Asia, to see how they could move fast leveraging both teams.

> *"Nevertheless, this platform is quite new in Landi and not all features are yet available : in particular,* ***swipe, audio jack interface & power management are not ready****. I'd like to discuss with you at Cartes & next week on how we could manage to* ***move fast leveraging both teams****. Liu Shying, R&D VP of Landi will be at Cartes on Wednesday & Thursday, I'd like to organize a discussion together on this opportunity." [email from C. Rotsaert to Ben Lo, Mar 26, 2012 - BBPOS_1682180-BBPOS_1682184]*

217. In his email, what Mr. Rotsaert refers to as "swipe" is the communication format and Data DUKPT method that BBPOS had successfully deployed. The "audio jack interface" refers to the polarity detection and automatic gain control features of the BBPOS product. And the "power management" refers to the battery saving trade secret that BBPOS designed.

218. Clearly, Mr. Rotsaert saw the value of having these features in the Landi product for reasons discussed below:

- Polarity Detection & Correction – this feature was necessary for using with the audio jack of mobile phones in order to prevent damage to the mobile phone and/or mPOS device.
- Power Management – this is a highly valued feature for any battery powered device regardless of whatever secondary power or charging capabilities are present. One of the more inconvenient / quality perception issues with battery powered devices is battery life. This feature extends the battery life and thus the reliability of the device.
- Auto Gain Control – the adaptive threshold is essential for reliable communication because each mobile phone has different characteristics in the way they process audio signals. Without this feature, a significant percentage of the transmission of the credit card swipes would fail using this channel.
- Communication format – These formats were difficult to design, some required repeated testing to establish the right transfer formats for the data coming from the swiper once retrieved from the card. Without this capability, Ingenico would not have been able to support customers using these formats with ROAMpay.
- Data DUKPT – This proprietary secure data transfer method was incorporated into the Ingenico product, and it was necessary to support communication formats 11 and 29, which were used by Ingenico after being introduced to them from BBPOS. Without this capability, Ingenico would not have been able to support customers using these formats with ROAMpay.

9 CONCLUSIONS

219. As described in detail in the above sections, I have formed the following conclusions.

220. None of the prior art Shamos referenced actually discloses the details of BBPOS' trade secrets and did not solve the same problems as addressed by BBPOS trade secrets.

221. Dr. Shamos' argument that they could have been reverse engineered is incorrect on 2 points. First, I have shown that some if not all aspects of the trade secrets could not have been reverse engineered. Second, there is no evidence to suggest that Ingenico solved these problems addressed by the trade secrets by reverse engineering. To the contrary, my analysis indicates that Ingenico solved their problems by using the BBPOS trade secrets which were provided directly to Roam and Ingenico.

222. None of the prior art identified for each of the trade secrets categories discloses the specific methods described by the BBPOS trade secrets. There was no analysis or evidence provided that suggests Ingenico used any of the methods disclosed by the prior art. Again, to the contrary, my analysis indicates that Ingenico solved their problems by using the BBPOS trade secrets which was provided directly to Roam and Ingenico.

223. Dr. Shamos is using hindsight to suggest what a person skilled in the field allegedly could have done with those references. It is my understanding that there is no support, and it is improper, to use that type of hindsight reconstruction for obviousness of trade secrets. Specifically, there is no evidence that such development actually took place utilizing either reverse engineering or prior art. In my opinion, Ingenico's need for BBPOS' trade secrets

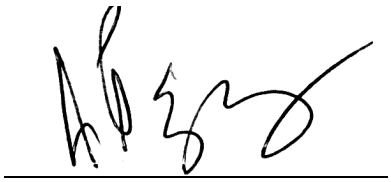
suggests that Ingenico was not able to solve its technical challenges without BBPOS' trade secrets.

10 CLOSING

224. Within a reasonable degree of professional certainty, I believe that Ingenico has misappropriated these 5 trade secrets they received from BBPOS to produce their iTMP product line including their RP350X, RP750X, RP100 series, and RP450 series products

225. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true.

Executed this 18th day of April, 2022.



Ivan Zatkovich

Exhibit A - CV of Ivan Zatkovich

Exhibit B – List of Materials

Exhibit C – Expert Report of Ivan Zatkovich